9

Databases for Non-EU Nationals and the Right to Private Life

Towards a System of Generalised Surveillance of Movement?

NIOVI VAVOULA

I INTRODUCTION

The creation of pan-European centralised databases that process the personal data of non-EU citizens is inextricably linked with the emergence of 'a Europe without internal frontiers'. The story begins in the mid-1980s with the evolution of European integration and the addition of borders to the list of responsibilities shared by the Member States and the EU (then European Community). In parallel, a more limited number of Member States decided to abolish their internal border controls within the framework of the so-called Schengen Agreement and Convention:[1] a person allowed to enter the territory of one of the participating countries was automatically permitted to circulate within the Schengen area, without being subjected again to checks at the border. As irregular migrants and criminals were not excluded from free circulation, the dismantlement of internal checks was accompanied by so-called compensatory or flanking measures providing for, among other things, a common set of rules on external borders, short-stay visas and asylum applications.[2] With the Treaty of Amsterdam, the law developed under the Schengen

[1] Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at their Common Borders, 14 June 1985, 2000 O.J. (L 239) 13 [hereinafter Schengen Agreement]; Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at their Common Borders, 19 June 1990, 2000 O.J. (L 239) 19 (signed 1990, entered into force 1993, applied 1995) [hereinafter CISA]. For parallel developments at EC level that led to the Schengen cooperation see Elspeth Guild, *European Community Law from a Migrant's Perspective* (The Hague: Kluwer, 2001), chapters 7–8.

[2] For the development of the Schengen *acquis* see Monica den Boer, ed., *Schengen, Judicial Cooperation and Policy Coordination* (Maastricht: European Institute of Public Administration, 1997).

https://doi.org/10.1017/9781108755641.009 Published online by Cambridge University Press

Convention, the so-called Schengen *acquis*, was integrated within EU law.[3] At the same time, the EU competence in Justice and Home Affairs (JHA) that had been introduced with the Maastricht Treaty was modified to include the overarching objective of establishing an Area of Freedom, Security and Justice (AFSJ).[4] Since then, a substantial corpus of legislation regulating access to, stay in and removal from the Schengen area has been progressively constructed.[5] Efforts to control the movement of non-EU nationals within the Schengen area have been coupled with efforts to prevent them from reaching the EU external border,[6] thus necessitating action outside the physical border.[7] In all of these developments, the growing tendency to associate non-EU nationals with irregular migration and criminality has been critical.

[3] Council Decision 1999/435/ EC, Concerning the Definition of the Schengen *Acquis*, 1999 O.J. (L 176) 1; Council Decision 1999/436/EC, Determining the Legal Basis for Each of the Provisions or Decisions which Constitute the Schengen *Acquis*, 1999 O.J. (L 176) 17. For an analysis see, among others, Eckart Wagner, "The Integration of Schengen into the Framework of the European Union," *Legal Issues of European Integration* 25, no. 2 (1998): 1–60; Pieter Jan Kuijper, "Some Legal Problems Associated with the Communitarization of Policy on Visas, Asylum and Immigration under the Amsterdam Treaty and Incorporation of the Schengen Acquis," *Common Market Law Review* 37, no. 2 (2000): 345–366.

[4] Article 61 Treaty Establishing the European Community and Article 2 Treaty on European Union [hereinafter TEU]. The Member States participating in the Schengen area and the AFSJ must be distinguished. The United Kingdom, Ireland and Denmark are non-Schengen States, but have the possibility to opt in to measures that develop those parts of the Schengen *acquis* that they subscribed to previously under their respective arrangements. Switzerland, Iceland, Norway and Liechtenstein are Schengen Associated States, without being EU Member States.

[5] A series of Schengen instruments have been recast as EU legislation, including the conditions under which a non-EU national may enter and reside on national territory. See European Parliament and Council Regulation (EU) 2016/399, On a Union Code on the Rules Governing the Movement of Persons across Borders (Schengen Borders Code), 2016 O.J. (L 77) 1. Furthermore, a Common European Asylum System (CEAS) setting common standards in administering applicants for international protection has been set up; this system includes rules on the Member State responsible for an asylum application, reception conditions, qualification and procedures. See Section II.1.2.

[6] Didier Bigo and Elspeth Guild, eds., *Controlling Frontiers: Free Movement into and within Europe* (Aldershot: Ashgate, 2005); Valsamis Mitsilegas, "Human Rights, Terrorism and the Quest for 'Border Security'," in *Individual Guarantees in the European Judicial Area in Criminal Matters*, eds. Marco Pedrazzi, Ilaria Viarengo, and Alessandra Lang (Brussels: Bruylant, 2011), 85–112; Valsamis Mitsilegas, "Immigration Control in an Era of Globalisation: Deflecting Foreigners, Weakening Citizens, Strengthening the State," *Indiana Journal of Global Legal Studies* 19, no. 1 (2012): 3–60; Valsamis Mitsilegas, "The Law of the Border and the Borders of Law: Rethinking Border Control from the Perspective of the Individual," in *Rethinking Border Control for a Globalizing World*, ed. Leanne Weber (Oxford: Routledge, 2015), 15–32.

[7] For an analysis see Bernard Ryan and Valsamis Mitsilegas, eds., *Extraterritorial Immigration Control* (Leiden: Martinus Nijhoff, 2010).

Asylum and visa applications, as well as entry and exit procedures, have been instrumentalised for the purpose of the prevention and investigation of crimes, particularly of terrorism.[8] More broadly speaking, security considerations have had a major impact in determining the objectives and rules of immigration control instruments.[9]

The evolution of digital technologies has been an indispensable component of these efforts, enabling the *en masse* storage and further processing of personal data collected on different groups of non-EU citizens. As Bonditti points out, technology has been the 'servant mistress of politics'[10] resulting in 'the digitalisation of the European migration policy'.[11] In this framework, technological advances, 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 legitimised at the border'.[12] Biometry in particular has been championed as a tool to reliably determine whether a third-country national is whom he claims to be.[13] The move to identify individuals based on their biological characteristics is attributed to a number of advantages of biometric over alphanumeric identifiers, including their universality, distinctiveness and permanence.[14]

Technological evolution has enabled the EU legislator to set up a 'mille-feuille' of information-processing schemes, currently comprising three

[8] For instance, the Hague Programme states: '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.' The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, 2004 O.J. (C 53) 1, 7.

[9] For instance, see Communication from the Commission, *The European Agenda on Security*, COM (2015) 185 final (28 April 2015).

[10] Philippe Bonditti, "From Territorial Spaces to Networks: A Foucaultian Approach to the Implementation of Biometry," *Alternatives: Global, Local, Political* 29, no. 4 (2004): 465–482.

[11] Michiel Besters and Frans Brom, "'Greedy' Information Technology: The Digitalization of the European Migration Policy," *European Journal of Migration and Law* 12, no. 4 (2010): 455–470.

[12] 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," *Citizenship Studies* 14, no. 1 (2010): 89–103.

[13] For a thorough analysis on biometrics see Els Kindt, *Privacy and Data Protection Issues of Biometric Identifiers* (Dordrecht: Springer, 2013).

[14] Anil Jain, Ruud Bolle, and Sharath Pankanti, *Biometrics. Personal Identification in Networked Society* (New York: Springer, 2006). For an analysis of implementing biometrics at the borders see European Commission, "Biometrics at the Frontiers: Assessing the Impact on Society," 2005, www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf. Their reliability has been criticised. See Elspeth Guild, Sergio Carrera and Alejandro Eggenschwiler, "Informing the Borders Debate," CEPS, 2009, 3, www.ceps.eu/system/files/book/1843.pdf.

large-scale information systems: the Schengen Information System (SIS II, formerly named SIS), which includes alerts on unwelcome third-country nationals, criminals and irregular migrants; Eurodac, where fingerprints are stored, primarily of asylum seekers; and the Visa Information System (VIS), which contains personal data collected from short-stay visa applicants. At present, the momentum for EU immigration databases is greater than ever. In addition to consecutive enhancements to the three existing databases, centralised systems are bound to proliferate via the establishment of an Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the European Criminal Record Information System for third-country nationals (ECRIS-TCN). Each system is set up as a network of databases, consisting of a central database, located in Strasbourg, and national databases in each participating Member State. Moreover, the different systems are established as separate entities. In view of this compartmentalisation, interoperability – different ways of linking information from the different data pots – is also in the pipeline.

This elaborate framework of databases exemplifies the gradual transformation of traditional immigration control to a system of mass surveillance of movement:[15] different groups of third-country nationals are classified according to the dangers they pose to society and surveillance techniques become the vehicle for managing these dangers. As Gammeltoft-Hansen has eloquently observed, EU immigration databases operate as a series of concentric 'risk filters' serving to categorise and identify migrants.[16] In this context, Broeders has framed immigration databases as forming part of 'panopticon Europe', an ever-growing strategy designed to exclude third-country nationals through delegitimatisation and criminalisation.[17] Bigo has instead coined the

[15] Annaliese Baldaccini, "Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases," *European Journal of Migration and Law* 10, no. 1 (2008): 31–49; Valsamis Mitsilegas, "Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance," in *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, eds. Elspeth Guild, Helen Toner, and Annaliese Baldaccini (Portland: Hart, 2007), 359–394; Valsamis Mitsilegas, "The Border Paradox: The Surveillance of Movement in a Union without Internal Frontiers," in *A Right to Inclusion and Exclusion? Normative Fault Lines of the EU's Area of Freedom, Security and Justice*, ed. Hans Lindahl (Oxford: Hart, 2009), 33–64. Clarke has coined the term 'dataveillance' to denote this type of surveillance through the collection of personal data. See Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms," *Roger Clarke's Website*, 15 August 1997.

[16] Thomas Gammeltoft-Hansen, "Filtering Out the Risk Migrant: Migration Control, Risk Theory and the EU," Working Paper 52/2006, AMID Working Paper Series 2006, 8.

[17] Dennis Broeders, "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants," *International Sociology* 22, no. 1 (2007): 71–92.

term 'banopticon', designed to highlight the fact that these systems are not intended to monitor everybody, but only the designated risk groups, constituting an exclusionary form of control that seeks to banish and prevent or deny entry.[18]

The aim of the present chapter is to map the landscape of pan-European centralised databases involving non-EU nationals by tracing three historical periods in the surveillance of movement: the initial, hesitant steps to employ technological means for purposes of immigration control; the systematisation of immigration databases and the gradual expansion of their capacities; and the current stage of generalised and normalised surveillance of movement through the processing of personal data on practically the entire non-EU population. Furthermore, as these many databases come into direct conflict with the rights to private life and personal data protection, this chapter offers an anthology of the issues of concern. The privacy guarantees and compliance standards are drawn from the jurisprudence of the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR), both of which have placed limits on mass surveillance, albeit in different factual contexts. Due to space constraints, the assessment focuses on the necessity of setting up or maintaining information systems, their personal scope, the categories of personal data processed (including biometric identifiers), access to stored data for law enforcement purposes and interoperability among the systems.

II THE THREE WAVES OF SURVEILLANCE OF MOVEMENT OF NON-EU NATIONALS

1 *The First Wave: Establishing Centralised Databases for the Purpose of Modernising Immigration Control*

In the early 1990s, the first EU immigration databases were created: the emblematic Schengen Information System (SIS) and Eurodac, designed to facilitate the allocation of responsibility for examining asylum applications among the Member States. At the time, the technology was still fairly rudimentary, and therefore these two databases necessarily followed a compartmentalised approach. In addition, compartmentalisation was framed as a means of safeguarding the limited purposes and personal scope of each

[18] Didier Bigo, "Globalized (In)Security: The Field and the Ban-Opticon," in *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, eds. Didier Bigo and Anastassia Tsoukala (Oxford: Routledge, 2008), 10–48.

database, thus conforming with one of the key principles of EU data protection law, the purpose limitation principle.[19]

1.1 Keeping Away the Unwanted: The SIS

Perhaps the best-known centralised database in the AFSJ is the SIS, which, as discussed later, has since been replaced by SIS II. At the heart of the compensatory measures for the abolition of internal border controls,[20] the SIS was conceived in 1987 and became operational in 1995.[21] The system held data categorised in the form of alerts on various categories of persons and objects, in particular on people (EU and non-EU nationals alike) wanted for arrest and extradition,[22] missing persons,[23] witnesses or persons summoned to appear before the judicial authorities or to serve a penalty,[24] persons or objects subject to discreet surveillance (where the individual is not made aware of the surveillance) or specific checks[25] and objects sought for the purpose of seizure or their use as evidence in criminal proceedings.[26] In addition, the SIS held alerts on non-EU nationals to be refused entry or stay in the Schengen area.[27] The variety of possible alerts reflected the system's overall purpose of ensuring a high level of security in the Schengen area by facilitating both border control and police investigations.[28] On the one hand, the SIS was meant to be used by national police, customs and border control authorities when performing checks on persons at their external borders or on national territory. On the other hand, it was designed to assist immigration officers when processing third-country nationals, particularly in relation to issuing visas

[19] According to the principle, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible to those purposes. See European Parliament and Council Regulation (EU) 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, art. 5(1)(b) [hereinafter General Data Protection Regulation].

[20] Bernd Schattenberg, "SIS: Privacy and Legal Protection," in *Free Movement of Persons in Europe: Legal Problems and Experience*, eds. Henry Schermers et al. (Dordrecht: Martinus Nijhoff, 1993), 43.

[21] For a detailed overview of the setting of the SIS see Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Leiden: Martinus Nijhoff, 2008), 47–57.

[22] Article 95 CISA.

[23] Article 97 CISA.

[24] Article 98 CISA.

[25] Article 99 CISA.

[26] Article 100 CISA.

[27] Article 96 CISA.

[28] Article 93 CISA.

and residence permits.[29] By its very (mixed) nature, the SIS thus served as both an immigration and a criminal law instrument.

In practice, alerts on third-country nationals dominated the system.[30] Data could be inserted on two main grounds.[31] First, alerts could be registered on the basis of public policy, public security or national security grounds.[32] This could be the case when third-country nationals had been convicted of an offence carrying a penalty involving deprivation of liberty for at least one year,[33] or there were serious grounds for believing that they had committed serious criminal offences, or there was clear evidence that they planned to commit such offences in the territory of a signatory state.[34] Second, alerts could be inserted with respect to third-country nationals who had not complied with national immigration law, on the basis of a deportation order or refusal of entry, including or accompanied by a prohibition on entry or a prohibition on residence.[35]In connection with each alert, the SIS stored basic alphanumeric information – name, nationality, the type of alert, any specific objective physical characteristics and so on – and operated on a hit/no hit basis. In the event of a hit, national authorities would perform searches for supplementary information in another system named Supplementary Information Request at the National Entries (SIRENE).[36]

[29] Article 92 CISA.

[30] Elspeth Guild, "Moving the Borders of Europe," Inaugural lecture, University of Nijmegen 2000, 24, http://cmr.jur.ru.nl/cmr/docs/oratie.eg.pdf; Brouwer, *Digital Borders and Real Rights*, 66–68; Schengen Joint Supervisory Authority, *Final Report of the Schengen Joint Supervisory Authority on the Follow-Up of the Recommendations Concerning the Use of Article 96 Alerts in the Schengen Information System* (26 November 2010).

[31] In the early days of the SIS, under Article 96 CISA all alerts were inserted at the discretion of national authorities, on the basis of a national decision either by an administrative or judicial authority.

[32] National security is understood as encompassing surveillance by the intelligence services of the Member States, particularly with regard to the fight against terrorism. Public security is not defined under EU law. Drawing from the case law on free movement law, public security covers both internal and external security (Case C-367/89, *Aimé Richardt and Les Accessoires Scientifiques SNC*, ECLI:EU:C:1991:376) and can involve a risk of serious disturbances to foreign relations or to the peaceful coexistence of nations (Case C-83/94, *Peter Leifer, Reinhold Otto Krauskopf and Otto Holzer*, ECLI:EU:C:1995:329). Furthermore, in *P.I.*, the term 'imperative grounds of public security' was interpreted as meaning 'a particularly serious threat to one of the fundamental interests of society, which might pose a direct threat to the calm and physical security of the population'. See Case C-348/09, *P. I.* v. *Oberbürgermeisterin der Stadt Remscheid*, ECLI:EU:C:2012:300.

[33] Article 96(2)(a) CISA.

[34] Article 96(2)(b) CISA.

[35] Article 96(3) CISA.

[36] Each Member State operates a SIRENE Bureau, available 24/7, responsible for any supplementary information exchange and coordination of activities connected to SIS alerts.

1.2 Monitoring the Territorial Belonging of Asylum Seekers and Irregular Migrants: Eurodac

Parallel to the establishment of the SIS and also in response to the abolition of border controls within the Schengen area, national governments set out common rules on how to determine which Member State would be responsible for examining individual asylum applications.[37] The Dublin Convention, which was signed in 1990 and entered into force in 1997,[38] allocated asylum applications to a single Member State based on prescribed hierarchical criteria. A necessary corollary was a central registration system that would process the fingerprints of asylum seekers and assist in the implementation of the Dublin system. Eurodac (standing for European Dactyloscopy), the first pan-European *biometric* database, was created by Regulations 2725/2000[39] and 407/2002[40] and became operational in 2003.[41] According to its basic rules, every asylum seeker over the age of fourteen must enter their fingerprints when they apply for international protection. The collected fingerprints are stored in its Central System and are compared with fingerprints that have already been transmitted by other participating countries.[42] As with the SIS, Eurodac functions on a hit/no hit basis; if a Eurodac check reveals that the

The SIS should thus be understood as an index, which enables national authorities, after a hit, to exchange further information stored in SIRENE.

[37] For a comprehensive analysis of EU asylum law and policy, see Chapter 8.

[38] Convention Determining the State Responsible for Examining Applications for Asylum Lodged in One of the Member States of the European Communities, 15 June 1990, 1997 O.J. (C 254) 1 [hereinafter Dublin Convention]. The Convention superseded the refugee section in CISA. It was later replaced by Council Regulation 343/2003, 2003 O.J. (L 50) 1 [hereinafter Dublin II Regulation] and European Parliament and Council Regulation (EU) 604/2013, 2013 O.J. (L 180) 31 [hereinafter Dublin III Regulation]. The Dublin IV Regulation is currently being negotiated. See *Proposal for a Regulation Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in One of the Member States by a Third-Country National or a Stateless Person*, COM (2016) 270 final (4 May 2016).

[39] Council Regulation (EC) 2725/2000, Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin Convention, 2000 O.J. (L 316) 1 [hereinafter Eurodac Regulation].

[40] Council Regulation (EC) 407/2002, Laying Down Certain Rules to Implement Regulation (EC) No 2725/2000 Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin Convention, 2002 O.J. (L 62) 1.

[41] For a detailed overview of the story behind Eurodac see Jonathan Aus, "Eurodac: A Solution Looking for a Problem?" *European Integration Online Papers* 10 (2006): 1–26; Steve Peers and Nicole Rogers, eds., *EU Immigration and Asylum Law* (Leiden: Martinus Nijhoff, 2006), 263–268; Niovi Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Databases* (Leiden: Brill, 2019), chapter 4.

[42] Eurodac Regulation, arts. 4–7.

fingerprints have already been recorded in another Member State, the asylum seeker may be sent to that Member State. In addition, the system processes the data of all migrants that are apprehended in connection with irregular border crossings by land, sea or air or that are found to be irregularly staying on the territory of a Member State.[43] This category of data is also connected with the operation of the Dublin system, as a key criterion for assigning responsibility among the Member States is the asylum seeker's country of first entry into the EU.[44] Storing the fingerprints of irregular migrants at the EU's external border enables national authorities to track the (possible) movement of asylum seekers prior to their lodging of an application.

As for the type of data stored in Eurodac, apart from a full set of fingerprints, it only contains limited biographical information. The person's name and nationality are not included and, thus, individuals are identified by no more than their fingerprints.[45] The fingerprints of asylum seekers are retained for a period of ten years, while those of individuals found irregularly entering for two years only (now eighteen months).[46] The fingerprints of migrants found irregularly staying are not centrally stored, but only compared on the spot with the existing Eurodac data for the sole purpose of determining whether the irregular migrant has formerly applied for international protection in another Member State.

2 *The Second Wave: Immigration Databases and the 'War on Terror'*

The events of 9/11 signalled a new era for pan-European immigration databases. In response to the terrorist attacks, policies on immigration control, public security and criminality have become extensively intertwined. The migration-risk nexus fuelled by the events in the United States, and then the attacks in Madrid (2004) and London (2005), coincided with technological advances, and the combination resulted in the creation of a new database and the expansion of old ones. As detailed in the following section, the VIS was

[43] Eurodac Regulation, arts. 8–10.

[44] Dublin III Regulation, art. 13.

[45] Elspeth Guild, "Unreadable Papers? The EU's First Experiences with Biometrics: Examining Eurodac and the EU's Borders," in *Are You Who You Say You Are? The EU and Biometric Borders*, ed. Juliet Lodge (Nijmegen: Wolf Legal Publishers, 2007), 32.

[46] See European Parliament and Council Regulation (EU) 603/2013, 2013 O.J. (L 180) 1 [hereinafter Recast Eurodac Regulation]. The Regulation is discussed later in this chapter, but it bears mentioning here that the retention period was only partially justified. According to Article 13(1) of the Dublin III Regulation, a Member State remains responsible as the first country of entry for a period of one year; there is no reason why the retention period is eighteen months rather than one year.

created for the administration of the common EU visa policy and the data of short-stay visa applicants. SIS (SIS II) was significantly expanded through the insertion of additional features and the collection and storage of biometrics. Eurodac was reformed to encompass not only the primary purpose of administering the asylum allocation system but also the ancillary purpose of assisting in the fight against terrorism and serious crime.

2.1 Targeting Visa Applicants: The VIS

Visas are an emblematic symbol of the state's right to control entry of aliens. They first became a matter of collective interest in the Schengen framework, which contained extensive rules on short-stay (Schengen) visas,[47] supplemented by provisions on freedom to travel.[48] With the entry into force of the Amsterdam Treaty, EU competences in the field of short-stay visas were significantly reinforced.[49] However, progress on establishing a common visa policy was rather slow until the events of 9/11. Immediately afterwards, the EU Member States decided to reform the EU common visa policy by establishing a network for information exchange among their national authorities responsible for issuing short-stay visas.[50] The underlying rationale was to reinforce extraterritorial immigration control by storing the personal data collected from visa applicants and, at the same time, to exploit this pool of information for law enforcement purposes. The premise was that visa applicants constitute a risky population not only for immigration-control purposes but also for crime prevention, justifying measures that would potentially pre-empt and deter their movement.[51] As was explicitly stated '(t)he events of 11 September 2001 ... radically altered the situation, showing that visas are not just about

[47] Articles 9–17 CISA. The duration of a short-stay is no more than three months in any six-month period from the date of first entry in the territory of the Member State.

[48] Articles 19–24 CISA.

[49] Articles 62(2)(b), 62(3), 67 Treaty Establishing the European Community. For an overview see Annalisa Meloni, "The Development of a Common Visa Policy under the Treaty of Amsterdam," *Common Market Law Review* 42, no. 5 (2005): 1357–1381.

[50] For an overview of the discussions see Council Document 12019/01 (20 September 2001); Council Document 14523/01 (26 November 2001); Council Document 15577/01 (21 December 2001); Council Document SN 300/1/01 (15 December 2001). On the emphasis on 'border security' see Valsamis Mitsilegas, "Borders, Security and the Transatlantic Cooperation in the Twenty-First Century: Identity and Privacy in an Era of Globalized Surveillance," in *Immigration Policy and Security*, eds. Terri Givens, Gary Freeman, and David Leal (New York: Routledge, 2009), 148–166.

[51] Louise Amoore and Marieke de Goede, eds., *Risk and the War on Terror* (Oxford: Routledge, 2008).

controlling immigration but are above all an issue of EU member states' internal security.'[52]

The VIS database was established by a series of instruments: Decision 2004/512/EC,[53] which formed the legal basis for the VIS; Regulation 767/2008[54] governing the use of the system for border control purposes; and Council Decision 2008/633/JHA[55] prescribing the modalities by which visa data was to be consulted by law enforcement authorities and Europol.[56] After numerous years of complications, the gradual rollout of the VIS concluded in February 2016.[57] The database operates in tandem with the EU rules on short-stay visas. The current legal framework comprises a 'black list' of countries whose nationals must be in possession of a visa prior to their entry in the Schengen area, the Visa Code prescribing procedures and standards for national authorities, and rules on the uniform format of visas. Long-stay visas remain regulated at the national level only.

The VIS database currently constitutes the largest information exchange scheme in the EU. As of 30 September 2017, the VIS contained over 49 million visa applications and almost 42 million fingerprint sets.[58] Reflecting the post-9/11 migration-risk nexus, the VIS is designed for multiple purposes. Article 2 of the VIS Regulation stipulates that the overarching purpose of the database is to improve the implementation of the common visa policy by facilitating the

[52] Council Document 14523/01 (26 January 2002).

[53] Council Decision 2004/512/EC, Establishing the Visa Information System (VIS), 2004 O.J. (L 213) 5.

[54] European Parliament and Council Regulation (EC) 767/2008, 2008 O.J. (L 218) 60 as amended by the European Parliament and Council Regulation (EC) 810/2009, Visa Code, 2009 O.J. (L 243) 1 [hereinafter VIS Regulation].

[55] Council Decision 2008/633/JHA, 2008 O.J. (L 218) 129 [hereinafter VIS Decision]. The need for different legal instruments reflects the (former) pillar structure under which rules on immigration and asylum matters were (in the vast majority of cases) adopted under co-decision between the European Parliament and the Council, whereas rules on judicial and police cooperation in criminal matters were subject to unanimity in the Council and mere consultation of the European Parliament.

[56] Europol is the EU Agency for Law Enforcement Cooperation aimed at supporting cooperation between domestic law enforcement authorities through the collection, storage, further processing, analysis and exchange of personal data, whether provided by Member States or produced by the agency itself. In operation since 1999, Europol is currently governed by the European Parliament and Council Regulation (EU) 2016/ 794, On the European Union Agency for Law Enforcement Cooperation (Europol) and Replacing and Repealing Council Decisions 2009/ 371/ JHA, 2009/ 935/ JHA, 2009/ 936/ JHA, and 2009/ 968/ JHA, 2016 O.J. (L 135) 53.

[57] Commission Implementing Decision (EU) 2016/281, Determining the Date from which the Visa Information System (VIS) Is to Start Its Operations at External Border Crossing Points, 2016 O.J. (L 52) 64.

[58] eu-LISA, Technical Reports on the Functioning of VIS (May 2018), 4.

exchange of short-stay visa data; however, it further sets out no fewer than seven sub-purposes.[59] In practice, the VIS is meant to be used in a variety of fora: when processing an application for a Schengen visa in a consulate; when verifying the identity of the visa holder at the border against the data stored in the system; when performing checks on national territory to verify the identity and status (visa holder, asylum seekers, irregular migrant) of a third-country national; and in the context of the prevention, detection or investigation of serious crimes.

The system stores a wide array of personal data of visa applicants, irrespective of whether their application has been granted, refused, revoked, renewed or discontinued. These data include bibliographic information, biometrics (a full set of fingerprints and a photograph), information on persons who have issued an invitation and/or are liable to pay for the applicant's subsistence costs, purpose of the travel, residence and occupation.[60] By including such extensive information on visa applicants, the VIS implies an element of suspicion of visa applicants – they need to be monitored even though they have an a priori legitimate reason for travel to the EU. Crucially, this shadow of suspicion accompanies not only the travellers as such but also the family members, organisations or companies that have issued invitations or sponsored a stay within the Schengen area. Everyday activities are transformed into risks to be managed and prevented by gathering an extensive array of private information and putting it in the hands of a wide range of domestic authorities.

Turning to data access, outside of immigration authorities, access to VIS data is not routinely granted. Law enforcement authorities are allowed access only when necessary in a specific case, and only when there are reasonable grounds to believe that consultation of the system will substantially contribute to the prevention, detection or investigation of terrorist offences and other

[59] These include: (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, which is meant to assist in cases when a visa applicant has applied for international protection, as according to the Dublin criteria the Member State that has granted a Schengen visa will be responsible and (g) Contributing to the prevention of threats to Member States' internal security. For a critical examination of the VIS purposes see Vavoula, *Immigration and Privacy in the Law of the European Union*, chapter 3. The ranking of the purposes has been subject to litigation before the EU Court of Justice. See Case C-482/08, *UK* v. *Council*, ECLI:EU:C:2010:631.

[60] VIS Regulation, art. 9.

serious crimes.[61] These conditions must be verified by the Member State's Central Access Point following a reasoned electronic request by the designated authority.[62] More ambiguously, access to VIS data by Europol is allowed 'within the limits of its mandate and when necessary for the performance of its tasks'.[63]

2.2 From the SIS to the SIS II: The Transformation of the System from a Reporting to an Investigation Tool

A second strand of action as regards the operation of immigration databases in the wake of the 9/11 events has been the reinforcement of the functions of the SIS. At a Spanish initiative, Regulation 871/2004[64] and Council Decision 2005/211/JHA[65] were adopted stipulating wider access to certain types of data by visa, judicial and law enforcement authorities, among which Europol and Eurojust were included.[66] In the case of Europol, however, access was not granted to immigration data. At the same time, it became obvious that there was a pressing need to develop a second generation SIS – the SIS II – to accommodate the expanded EU family after the 2004 enlargement. The migration from the SIS to the SIS II was also regarded as a first-class opportunity to insert new functionalities into the system by taking advantage of the latest developments in the field of information technology.[67] Two Regulations and a Decision were formally adopted in 2006;[68] due to numerous technical complications the SIS II only commenced its operation in April 2013.

[61] VIS Decision, art. 5(1).
[62] VIS Decision, art. 4.
[63] VIS Decision, art. 7.
[64] Council Regulation (EC) 871/2004, Concerning the Introduction of Some New Functions for the Schengen Information System, Including in the Fight against Terrorism, 2002 O.J. (L 162) 29.
[65] Council Decision 2005/211/JHA, Concerning the Introduction of Some New Functions for the Schengen Information System, Including in the Fight against Terrorism, 2005 O.J. (L 68) 44.
[66] Eurojust is the counterpart of Europol in relation to judicial cooperation. See Council Decision 2009/426/JHA, On the Strengthening of Eurojust and Amending Decision 2002/187 JHA Setting Up Eurojust with a View to Reinforcing the Fight against Serious Crime, 2009 O.J. (L 138) 14.
[67] 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.
[68] European Parliament and Council Regulation (EC) 1987/2006, On the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II), 2006 O.J. (L 381) 4 [hereinafter SIS II Regulation]; Council Decision 2007/533/JHA, On the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II), 2007 O.J. (L 205) 63 [hereinafter SIS II Decision]; European Parliament and Council

The reforms made to the SIS II signal its gradual transformation from a mere reporting mechanism to a general investigation tool.[69] In this respect, one major shift has been the possibility of interlinking alerts involving different individuals or events that are inserted under different legal bases.[70] Such interlinking is allowed only if there is a clear operational need. Whether or not the option is used is subject to the national law of the public authority's Member State, which raises the prospect of the creation of significantly different systems across the EU. The potential for profiling through the interlinking of alerts is significant: 'the 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',[71] which may lead to their being treated with greater suspicion if they are deemed to be associated with criminals or wanted persons. Even though authorities with no right of access to certain categories of alert will not be able to see the link to an alert to which they do not have access, for instance motor vehicle authorities with respect to immigration alerts, such authorities will not necessarily be unaware of the existence of a link.[72]

Another major change involves the possibility of including biometric identifiers (photographs and fingerprints) within the system.[73] This change is part of a more general trend to introduce biometrics in all EU databases and documents: as described previously, both VIS and Eurodac are based on the collection and storage of biometrics; EU rules on the format for residence

Regulation (EC) 1986/2006, Regarding Access to the Second Generation Schengen Information System (SIS II) by the Services in the Member States Responsible for Issuing Vehicle Registration Certificates, 2006 O.J. (L 381) 1. On the need for separate instruments see Note 55.

[69] For the sake of a holistic approach it must be noted that under the revised SIS II rules, the registration of alerts on public policy, public security and national security grounds became mandatory. See SIS II Regulation, art. 24.

[70] Examples of interlinking include: (a) an EU national wanted for arrest based on a European Arrest Warrant related to a convicted companion who should be refused entry; (b) family members in respect of whom SIS II alerts have been registered; (c) a third-country national parent who should be refused entry related to a missing child (third-country national); (d) a third-country national to be refused entry and the possibility of them being a witness in an illegal immigration case; (e) a husband convicted criminal to be refused entry whose wife is a suspected terrorist; (f) a third-country national to be refused entry who is also a suspect in an illegal immigration case; (g) a third-country national to be refused entry using his or her own car, boat or aircraft; and (h) a third-country national to be refused entry using a stolen identity document. Council Document 12573/3/04 (30 November 2004), 3.

[71] Opinion of the European Data Protection Supervisor, 2006 O.J. (opinion on proposed SIS II regulations and decision).

[72] Valsamis Mitsilegas, *EU Criminal Law* (Oxford: Hart, 2009), 241.

[73] SIS II Regulation, art. 22.

permits and EU passports also require the use of biometrics.[74] According to Article 22 of the SIS II Regulation, biometrics will be introduced in two phases: (i) in the first stage, they will be used only for identity verification by comparing the biometric identifiers of the person of interest with those – and only with those – existing in the SIS II under that person's name (one-to-one searches); (ii) the second stage would allow the use of the biometrics to identify other individuals of interest (one-to-many searches). This development has significant implications: it transforms the database into a general intelligence weapon, as biometrics can be used in the course of investigations to conduct speculative searches in the database's pool of suspected population – so-called fishing expeditions.[75] In this respect, biometrics will operate as a vital search key for revealing links to other alerts. A Commission report on the readiness and availability of fingerprints for identification purposes confirms these concerns, as it is stated that a comparison of fingerprints with those already stored 'might identify links with other alerts'.[76] In sum, biometrics are not merely collected and stored to sort out the 'welcome' from the 'unwanted' but also to enhance the investigative powers of national law enforcement authorities.

2.3 The Use of Eurodac Data for Law Enforcement Purposes

A paradigmatic example of how the boundaries between immigration and police databases have been blurred and how the specified purpose of personal data collection no longer serves as a limit on data processing activities is the reconfiguration of Eurodac from a tool serving the Dublin system to a weapon in the fight against terrorism and serious crime. A year after the database had begun its operation, the Hague Programme called for the maximisation of effectiveness and interoperability of EU information systems and 'an innovative approach to the cross-border exchange of law enforcement information'.[77] Shortly afterwards, the Commission published a Communication on

[74] Evelien Brouwer, "The Use of Biometrics in EU Databases and Identity Documents: Keeping Track of Foreigners' Movements and Rights," in *Are You Who You Say You Are? The EU and Biometric Borders*, ed. Juliet Lodge (Nijmegen: Wolf Legal Publishers, 2007), 45–66; Baldaccini, "Counter-Terrorism and the EU Strategy for Border Security."

[75] Ben Hayes, "From the Schengen Information System to the SIS II and the Visa Information System (VIS): The Proposals Explained," Statewatch, February 2004, 4; Baldaccini, "Counter-Terrorism and the EU Strategy for Border Security," 38.

[76] Report from the 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)*, COM (2016) 93 final (29 February 2016), 7.

[77] See The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, 7.

improved effectiveness, enhanced interoperability and synergies of EU information systems 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'.[78] After four proposals and largely under the pressure of finalising the second phase of the Common European Asylum System (CEAS),[79] the recast Eurodac Regulation was adopted in June 2013,[80] allowing consultation of asylum seekers' fingerprints for the purposes of prevention, detection and investigation of terrorist offences and other serious crimes.

As with the VIS, law enforcement access is listed as an ancillary purpose; the principal purpose remains that of supporting the implementation of the Dublin asylum rules. Following the VIS model, consultation of Eurodac data does not take place on a routine basis and involves only the prevention, detection and investigation of terrorist offences and other serious crimes.[81] The conditions for access are somewhat stricter than the ones prescribed in the VIS Decision.[82] There is an additional step for accessing the Eurodac data: the national authority must have already consulted national fingerprint databases, as well as the automated fingerprinting identification systems (AFIS) of other Member States[83] and the VIS, and such consultation must have proven futile.[84] This step is meant to ensure that consultation of Eurodac is reserved only for cases in which other pools of information have been exhausted. Furthermore, compared to VIS, the necessity of consulting the database is defined more carefully: according to Article 20(1)(b), 'there must be an overriding public security concern which makes the searching of the database

[78] Communication from the Commission, *Improved Effectiveness, Enhanced Interoperability and Synergies among European Databases in the Area of Justice and Home Affairs*, COM (2005) 597 final (11 November 2005).

[79] See Brigitta Juster and Vassilis Tsianos, "Erase Them! Eurodac and Digital Deportability," *Transversal/EIPCP Multilingual Webjournal*, February 2013, http://eipcp.net/transversal/0313/kuster-tsianos/en.

[80] See Recast Eurodac Regulation.

[81] Recast Eurodac Regulation, recital 31. See Opinion of the European Data Protection Supervisor, 2013 O.J. (C 28) 3, para. 54 (opinion on proposal for recast Eurodac, executive summary); Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), Note on the Proposal for a Regulation on the Establishment of Eurodac (COM(2012)254), CM1216 (2012).

[82] These conditions apply also in the case of Europol access to Eurodac data.

[83] Such consultation is conducted on the basis of Council Decision 2008/615/JHA, On the Stepping up of Cross-Border Cooperation, Particularly in Combating Terrorism and Cross-Border Crime, 2008 O.J. (L 210) 1 [hereinafter Prüm Decision].

[84] Recast Eurodac Regulation, art. 20(1). There is a caveat: Article 20(1) prescribes that prior consultation is not necessary if there are reasonable grounds to believe that a comparison with such systems would not lead to the establishment of the identity of the data subject.

proportionate'. Verification that these data access conditions have been met is entrusted to a verifying authority assigned at the national level.

3 *The Third Wave: The Generalisation of Surveillance of Movement of Non-EU Citizens*

The most recent burst of database activity has been prompted by the terrorism events in France in November 2015 and Belgium in March 2016. A number of proposals that had remained in the EU legislative drawer for years, successfully opposed by those against normalising surveillance of movement,[85] re-emerged as part of a comprehensive, multi-faceted response at EU level, encapsulated in the concept of establishing a 'genuine Security Union'.[86] Dossiers that were particularly contentious in the past (Entry/Exit System and European Travel Information and Authorisation System [ETIAS]) have been prioritised and speedily adopted. At the same time, existing databases have been re-jigged to explicitly encompass security considerations.[87] Overall, the development of pan-European immigration databases has accelerated tremendously: new systems have been established to fill perceived 'informational gaps' created by the compartmentalised approach of the 1990s and 2000s; the existing systems have been reformed to enhance and magnify their use and effectiveness; and interoperability has been heavily promoted, to enable the connection of the 'data pots' in a variety of ways.

3.1 Visa-Free Travellers as a Risk: The Establishment of the EES and the ETIAS

Although the databases discussed previously in the chapter create a rather comprehensive network of information exchange schemes concerning third-country nationals, they do not cover those originating from countries not subject to the visa regime. Influenced by similar initiatives in the United States, particularly the US-VISIT programme (now IDENT), the European Council hinted at this 'informational gap' in the Hague Programme[88] and so

[85] Valsamis Mitsilegas and Niovi Vavoula, "The Normalisation of Surveillance in an Era of Global Mobility," in *Handbook of Migration and Security*, ed. Philippe Bourbeau (Cheltenham: Edward Elgar, 2017), 232–251.

[86] See Communication from the Commission, COM (2015) 185 final.

[87] Communication from the Commission, *Stronger and Smarter Information Systems for Borders and Security*, COM (2016) 205 final (6 April 2016).

[88] See The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, 7.

too did the Commission in its Communication on improved effectiveness, enhanced interoperability and synergies among information systems.[89] After years of discussions,[90] in 2013 the Commission presented three legislative proposals commonly referred to as the 'Smart Borders Package'. This Package was composed of a proposal to establish the EES at the EU external borders,[91] a proposal for a 'Registered Travellers Programme' (RTP) to facilitate the border crossing of pre-screened *bona fide* travellers,[92] and one on amendments to the Schengen Borders Code to reflect the changes.[93] Due to proportionality concerns,[94] the Commission originally left the registration of biometrics and law enforcement access outside the scope of that proposal, and later entirely withdrew the package and committed to submitting revised proposals in early 2016. However, in the aftermath of the 2015 terrorist events, the EES rose high on the EU agenda, including a far-reaching proposal to further extend the reach of the EES to cover EU nationals.[95] The EES was ultimately adopted in November 2017 and certain rules were slightly modified, but the basic policy choices remained the same.[96] The idea of the RTP was abandoned.

The system is designed to register border crossing both at entry and exit for all non-EU nationals admitted for a short stay, irrespective of whether they are required to obtain a Schengen visa or not.[97] It will also apply to non-EU nationals whose entry for a short stay has been refused at the border, which

[89] See Communication from the Commission, COM (2005) 597 final, 9.

[90] Vavoula, *Immigration and Privacy in the Law of the European Union*, chapter 5.

[91] *Commission Proposal for a Regulation of the European Parliament and of the Council Establishing an Entry/Exit System (EES) to Register Entry and Exit Data of Third Country Nationals Crossing the External Borders of the Member States of the European Union*, COM (2013) 95 final (28 February 2013).

[92] *Commission Proposal for a Regulation of the European Parliament and of the Council Establishing a Registered Traveller Programme*, COM (2013) 97 final (28 February 2013).

[93] *Commission Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 562/2006 as Regards the Use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP)*, COM (2013) 96 final (28 February 2013).

[94] For criticism, see among others Opinion of the European Data Protection Supervisor, 2014 O.J. (C 32) 25 (executive summary); Article 29 Data Protection Working Party, Opinion 05/2013 on Smart Borders, WP206 (6 June 2013); Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), Note on the Smart Borders proposals (COM(2013) 95 final, COM(2013) 96 final and COM(2013) 97 final), CM1307 (3 May 2013).

[95] Council Document 12272/15 (25 September 2015).

[96] European Parliament and Council Regulation (EU) 2017/2226, 2017 O.J. (L 327) 20 [hereinafter EES Regulation].

[97] According to Article 2(3) of the EES Regulation, there are a few exceptions for non-EU nationals: those who have residence permits; are family members of an EU national and hold a residence card; or are family members of another non-EU national who enjoys free movement rights or has a residence card.

means that even though these persons will be physically kept outside of the EU, their data will be stored in the EES for future use. Following the VIS model, the EES is a multi-purpose tool: it will enhance the efficiency and automation of border checks; assist in the identification of irregular migrants; allow the identification and detection of overstayers; allow refusals of entry to be checked electronically; enable visa authorities to check the use of previous visas; inform non-EU nationals of the duration of their authorised stay; gather statistics; combat identity fraud and misuse of travel documents; and strengthen internal security and the fight against terrorism by allowing law enforcement authorities access to travel history records.[98] To these ends, once the system becomes operational, it will record the identities of third-country nationals, by storing alphanumeric data, four fingerprints and a facial image, along with details of their travel documents, which will be linked to electronic entry and exit records.[99] The retention periods foreseen vary depending on whether an exit record exists or not; if so, it is three years, but in case of *potential* overstayers, the records will be kept for five years.[100] The current practice of stamping travel documents will be abolished. Instead, the system will automatically calculate the maximum term of authorised stay in accordance with the Schengen Borders Code.[101] An information mechanism will be included to identify cases where there are no records of exit.[102] Access to EES data for the purposes of the prevention, detection and investigation of terrorist offences and other serious crimes is envisaged under a mixture of rules combining the Eurodac and the VIS models.[103] For example, verification that the conditions of access have been met is the responsibility of each Member State's Central Access Point; intelligence services are not excluded from accessing the EES data.[104] Furthermore, the EES Regulation allows national authorities to search the database to identify 'an unknown suspect perpetrator or suspected victim of a terrorist offence or other serious criminal offence' if they meet the listed conditions and have already (unsuccessfully) consulted their national databases or, in the case of fingerprints, their national AFIS.[105]

[98] EES Regulation, art. 6(1).
[99] EES Regulation, arts. 14–20.
[100] EES Regulation, art. 34.
[101] See Note 5.
[102] EES Regulation, art. 12.
[103] EES Regulation, arts. 29–33.
[104] EES Regulation, art. 29. Compare with Article 3 of the VIS Decision.
[105] EES Regulation, art. 32(2). Compare with Article 20(1) of the Eurodac Regulation.

The movement of visa-free travellers will also be monitored through the European Travel Information and Authorisation System (ETIAS), enacted in September 2018.[106] The ETIAS was initially conceptualised alongside the EES, with the Commission briefly mentioning that it would examine the possibility of introducing an Electronic System of Travel Authorisation (ESTA) to pre-screen non-EU nationals. The system, which was a transplantation of the US standards in the EU context, foresaw the pre-screening of non-EU nationals who were not subject to a visa requirement in order to verify that they fulfilled the entry conditions before travelling to the EU.[107] In 2011, the project was shelved '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'.[108] Nonetheless, following the removal of numerous countries from the 'black' list of countries whose nationals require a visa to enter the Schengen territory and under the influence of the 2015/2016 terrorist events, the idea re-emerged.[109] Reminiscent of the SIS II, the ETIAS Regulation solidifies the link between immigration control and security, as one of its main objectives is to contribute to a high level of security by thoroughly assessing whether travellers pose a 'security risk'.[110] There are many other purposes of the database: preventing illegal migration, protecting public health, enhancing the effectiveness of border checks, supporting the SIS II, and contributing to the prevention, detection and investigation of terrorist offences or of other serious criminal offences.[111]

To achieve these aims, all visa-exempt travellers shall be obliged to obtain authorisation prior to their departure through an online application in which they must disclose a series of personal data including biographical data, travel arrangements, home and email address, phone number, level of education and current occupation.[112] The pre-screening and provision of authorisation

[106] European Parliament and Council Regulation (EU) 2018/1240, 2018 O.J. (L 61) 1.

[107] Communication from the Commission, *Preparing the Next Steps in Border Management*, COM (2008) 69 final (13 February 2008); see also Commission, "Policy Study on an EU Electronic System for Travel Authorisation," Price Waterhouse Coopers, February 2011.

[108] Communication from the Commission, *Smart Borders – Options and the Way Ahead*, COM (2011) 680 final (25 October 2011), 7.

[109] Communication from the Commission, COM (2016) 205 final, 13.

[110] See European Parliament and Council Regulation (EU) 2018/1240, Establishing a European Travel Information and Authorisation System (ETIAS), 2018 O.J. (L 236) 1, art. 4(a) [hereinafter ETIAS Regulation]. According to Article 3(6), security risk is defined as the risk of a threat to public policy, internal security or international relations for any of the Member States.

[111] See ETIAS Regulation, art. 4(b)–(f).

[112] ETIAS Regulation, art. 17.

shall take place on the basis of automated processing[113] (comparison) of the applicant's personal data with three elements: (a) data held in existing immigration and law enforcement databases;[114] (b) screening rules *enabling profiling* on the basis of risk indicators, consisting of a combination of data including age range, sex, nationality, residence, level of education and occupation;[115] and (c) a special ETIAS watch list of individuals suspected of having participated in terrorism or other serious crimes or in respect of whom there are factual indications or reasonable grounds to believe that they will commit such offences.[116] In practice, the ETIAS will be used both at the borders by carriers and border authorities and by immigration authorities to verify travel documentation.[117] If authorisation is granted, data will be held for three years; otherwise, it will be held for five years.[118] Law enforcement authorities and Europol will be granted access under rules largely mirroring those in the VIS Decision.[119]

The EES and the ETIAS introduce mobility surveillance for almost all travellers. They are grounded on automaticity and almost blind reliance on technology.[120] As with the earlier databases, they are based on the collection and further processing of biometrics and they reinforce the link between immigration control and law enforcement. In many respects, the value and significance of short-stay (Schengen) visas are diminished: on the one hand, individuals who have obtained a visa are surveilled not only in the VIS but also in the EES; on the other hand, nationals from visa-exempt countries are nonetheless placed under suspicion, because they will soon be monitored in the EES and the ETIAS. This complex framework of consecutive surveillance of movement strongly supports the idea that all non-EU nationals are suspicious and form part of the risky population. In other words, in the eyes of the EU legislator, every non-EU national potentially constitutes a 'security risk'.

[113] The automated processing will be handled by the Central Unit, but in cases of a hit, manual processing will follow by the National Unit of the Member State responsible. See ETIAS Regulation, art. 26.

[114] These are: SIS II, VIS, Eurodac, EES, Europol database, the Interpol Stolen and Lost Travel Document Database, the Interpol Travel Documents Associated with Notices Database and the ETIAS.

[115] ETIAS Regulation, art. 33.

[116] ETIAS Regulation, art. 34.

[117] ETIAS Regulation, arts. 45–49.

[118] ETIAS Regulation, art. 54.

[119] ETIAS Regulation, arts. 50–53.

[120] See Article 20 of the EES Regulation about the rebuttable presumption of irregularity in lack of an exit record.

To conclude this discussion, it bears highlighting that the ETIAS will constitute as large a database as the EES and will contain as much personal information as the VIS, thus combining the worst of both worlds. Based on the ETIAS data, the authorities will be able to construct complete profiles of visa-exempt travellers who are previously unsuspected of any offence. Even though no biometrics will be stored, the categories of data collected and stored are quite extensive. Coupled with the EES, the ETIAS will constitute both a massive catalogue of third-country nationals and a powerful surveillance tool driven by the logic of risk prevention transplanted once again into immigration control.[121] Importantly, the ETIAS is understood as a platform for mining and profiling personal data, not simply issuing automated or manual travel authorisation decisions. The ETIAS screening rules are meant to identify persons who are otherwise unknown to national competent authorities but are *assumed* to be of interest for immigration control or security purposes and therefore are *likely* to commit criminal offences in the future. These persons will be flagged not because of any specific actions they have engaged in but because they display particular category traits in a probabilistic logic devoid of concrete evidence.[122]

3.2 The SIS II, Eurodac and VIS under Refurbishment

Efforts to fill in 'informational gaps' have been accompanied by radical reforms to all three operational databases. The Eurodac proposal was tabled in May 2016 and political agreement has been reached, even though formal adoption is still pending due to complications in other asylum-related files.[123] The proposal signals a landmark change in Eurodac's purpose – from a system aimed at the effective implementation of the Dublin mechanism into an instrument for *wider immigration purposes*, including the return of irregular migrants. The anticipated Eurodac reform is both quantitative and qualitative. Quantitavely, the scope *ratione personae* has been expanded and additional categories of data, including sensitive ones, are to be entered into the system. In particular, on top of a full set of fingerprints, Member States shall be obliged to take and transmit a facial image.[124] The age threshold for

[121] Vavoula, *Immigration and Privacy in the Law of the European Union*, chapter 6.
[122] Susie Alegre, Julien Jeandesboz, and Niovi Vavoula, *European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection*, Study for the European Parliament, PE 583.148, 2017, 23–26.
[123] *Commission Proposal for a Regulation of the European Parliament and of the Council*, COM (2016) 272 final (4 May 2016).
[124] *Commission Proposal*, COM (2016) 272 final, art. 2(1).

fingerprinting children is significantly reduced to the age of six.[125] 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'.[126] Furthermore, for the first time since the establishment of the database, information on persons who are found irregularly present on the national territory will be centrally stored.[127] As these new categories of persons and information suggest, the transformation is also qualitative: Eurodac has been detached from its original Dublin context and re-conceptualized as a multi-purpose immigration tool.

The SIS II also underwent a refurbishment.[128] The Commission proposal of December 2016 followed an evaluation of the system, which found that a major flaw was the lack of harmonised national criteria for entering alerts.[129] Regulations 2018/1860 and 2018/1861 rectify this issue, albeit taking the lowest-common-denominator approach and making the registration of entry bans and return decisions mandatory.[130]

As for the contemplated VIS reform, it is of perhaps greatest interest for the purposes of the present chapter. This is because it seeks to fill the one outstanding gap in the coverage of third-country nationals in EU databases[131] – holders of residence permits, residence cards and long-stay visa holders.[132] The

[125] *Commission Proposal*, COM (2016) 272 final, art. 2(2).
[126] *Commission Proposal*, COM (2016) 272 final, art. 13.
[127] See *supra*, section II.1.2.
[128] *Proposal for a Regulation of the European Parliament and of the Council on the Establishment, Operation and Use of the Schengen Information System (SIS) in the Field of Border Checks*, COM (2016) 882 final (12 December 2016); *Proposal for a Regulation of the European Parliament and of the Council on the Establishment, Operation and Use of the Schengen Information System (SIS) in the Field of Police Cooperation and Judicial Cooperation in Criminal Matters*, COM (2016) 883 final (21 December 2016); *Proposal for a Regulation of the European Parliament and of the Council on the Use of the Schengen Information System for the Return of Illegally Staying Third Country Nationals*, COM (2016) 881 final (21 December 2016) [hereinafter collectively SIS II Proposal].
[129] *Commission Proposal for a Regulation of the European Parliament and of the Council*, COM (2018) 882 final (12 December 2016); *Commission Proposal for a Regulation of the European Parliament and of the Council*, COM (2018) 883 final (12 December 2016); *Commission Proposal for a Regulation of the European Parliament and of the Council*, COM (2018) 881 final (12 December 2016).
[130] European Parliament and Council Regulation (EU) 2018/1860, On the Use of the Schengen Information System for the Return of Illegally Staying Third-Country Nationals, 2018 O.J. (L 312) 1, art. 3; European Parliament and Council Regulation (EU) 2018/1861, On the Establishment, Operation and Use of the Schengen Information System (SIS) in the Field of Border Checks, 2018 O.J. (L 312) 14, art. 24.
[131] Communication from the Commission, COM (2016) 205 final, 3.
[132] For the discussion on the merits of registering residence permit holders see Council Document 12527/15 (8 October 2015).

VIS proposal[133] would extend the system to these groups of non-EU nationals as well as lower the threshold age for fingerprinting (six years). With this reform, *almost all* third-country nationals will be monitored. The only exception will be family members of EU nationals who hold residence cards and thus benefit from free movement rights. The underlying logic for including legal residents and long-stay holders is the need to manage a decentralised system of residence permits issued at the national level, but this decentralised structure has been deemed to have a collateral effect on immigration control *and security*.[134] In particular, the inability to verify biometrically the identities of residence card and long-stay visa holders is considered a security risk.

3.3 The ECRIS-TCN: Bridging Law Enforcement with Immigration Control and Non-EU with EU Nationals?

The European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN) was proposed in June 2017.[135] This system emerged as a necessity purely in the law enforcement context, as in order to obtain complete information on previous convictions of non-EU nationals, requesting Member States were obliged to send 'blanket requests' to all Member States, thus creating a heavy administrative burden.[136] The ECRIS-TCN will be a centralised system for the exchange of criminal records on convicted third-country nationals and stateless persons and is meant to complement the already existing, decentralised ECRIS system through which information on the criminal records of EU nationals is exchanged among Member States.[137]

[133] *Commission Proposal for a Regulation of the European Parliament and of the Council*, COM (2018) 302 final (16 May 2018).

[134] See *Commission Proposal*, COM (2018) 302 final, art. 1(2).

[135] *Commission Proposal for a Regulation of the European Parliament and of the Council*, COM (2017) 344 final (29 June 2017); *Commission Proposal for a Directive of the European Parliament and of the Council*, COM (2016) 7 final (19 January 2016).

[136] Until now exchange of criminal records on non-EU nationals has been taking place under Council Decision 2009/316/JHA, On the Establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, 2009 O.J. (L 93) 33; Council Framework Decision 2009/315/JHA, On the Organisation and Content of the Exchange of Information Extracted from the Criminal Record between Member States, 2009 O.J. (L 93) 22.

[137] European Parliament and Council Regulation (EU) 2019/816, Establishing a Centralised System for the Identification of Member States Holding Conviction Information on Third-Country Nationals and Stateless Persons (ECRIS-TCN) to Supplement the European Criminal Records Information System and Amending Regulation (EU) 2018/1726, 2019 O.J. (L 135) 1 [hereinafter ECRIS-TCN Regulation]; European Parliament and Council Directive 2019/884, Amending Council Framework Decision 2009/315/JHA, as Regards the Exchange of Information on Third-Country Nationals and as Regards the European Criminal Records

In cases where a record exists, data will be transferred by the convicting Member State to the requesting Member State on a bilateral basis, as per the rules in the ECRIS. All queries will be submitted through the central ECRIS-TCN system, which will contain biographical and biometric data; the retention period is not universal and will depend upon the retention period for the criminal records in the national databases. A particularly thorny issue in the negotiations involved the inclusion of dual nationals, that is, EU citizens who also hold the nationality of a third State, which creates potential discrimination compared to other EU citizens.[138] The final text formally adopted in April 2019 indeed prescribes that the personal scope of the system includes 'citizens of the Union who also hold the nationality of a third country'.[139] Like the possibility raised in some quarters of expanding the EES to EU nationals, the ECRIS-TCN illustrates how data on EU nationals can make their way into databases for non-EU nationals.

3.4 Compartmentalisation Is Dead! Long Live Interoperability

With all non-EU nationals effectively captured by at least one database, the final step towards an EU 'Big Brother' is the interconnection of the different 'data pots' under the umbrella term of interoperability.[140] The interoperability debates first started in the aftermath of 9/11.[141] In its 2005 Communication, 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'.[142] However, details on the legal aspect of interoperability were spared, as the concept was reduced to a technical rather than a legal or political matter.[143] Since the Paris attacks of 13 November 2015, the

Information System (ECRIS), and Replacing Council Decision 2009/316/JHA, 2019 O.J. (L 151) 143.

[138] See Council Document 10828/18 (10 July 2018), where it is mentioned that the proposed solution would involve the registration of both dual nationals and non-EU nationals.

[139] ECRIS-TCN Regulation, art. 2.

[140] For an analysis of interoperability from the perspective of improving internal security, see Chapter 10.

[141] Council Document 13176/01 (24 October 2001).

[142] Communication from the Commission, COM (2005) 597 final.

[143] For a critique see Paul De Hert and Serge Gutwirth, "Interoperability of Police Databases within the EU: An Accountable Political Choice?" *International Review of Law Computers & Technology* 20, no. 1–2 (2006): 21–22; European Data Protection Supervisor, Comments on the Communication of the Commission on interoperability of European databases (10 March 2006).

connection of the 'data jars' has gained fresh impetus,[144] leading to the introduction of two proposals[145] which have recently been adopted.[146]

Interoperability is conceived as information systems 'speaking to each other' and as an evolutionary tool that will enable further uses through the aggregation of data from different sources. Its four main components are a European Search Portal (ESP), a shared Biometric Matching Service (BMS), a Common Identity Repository (CIR) and a Multiple Identity Detector (MID). The ESP will enable competent authorities to simultaneous query the underlying systems and the combined results will be displayed on one single screen. Even though the screen will indicate in which databases the information is held, access rights will remain unaltered and will proceed following the rules of each database.[147] The BMS will generate and store templates from all biometric data recorded in the underlying systems,[148] thus effectively becoming a new database that compiles biometrics from the SIS II, VIS, Eurodac, EES and ECRIS-TCN and that will replace separate searches in the other databases. At the core of interoperability lies the CIR, which will store an individual file for each person registered in the systems, containing both biometric and biographical data as well as a reference indicating the system from which the data were retrieved.[149] CIR's main objectives are to facilitate identity checks of third-country nationals,[150] assist in the detection of individuals with multiple identities and streamline law enforcement access. With respect to law enforcement, the rules explained earlier are substituted by a two-step process in which law enforcement authorities can first consult all databases to check whether records on an individual exist in any of the

[144] European Council, Conclusions, EUCO 28/15 (18 December 2015), 3; Council Document 7371/16 (24 March 2016), pt. 55. A High Level Expert Group on Information Systems and Interoperability was appointed and it delivered its final report in May 2017. The report gave the green light to implementing a number of aspects of interoperability, but interconnectivity was dismissed. See High Level Expert Group on Information Systems and Interoperability, Final Report (May 2017), http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

[145] One part of the legislative package deals with the databases that build on the Schengen Acquis, namely the EES, the VIS, ETIAS and those parts of SIS II that deal with border control cooperation. The other part covers Eurodac, the law enforcement aspects of the SIS II and the ECRIS-TCN.

[146] European Parliament and Commission, Regulation (EU) 2019/817, 2109 O.J. (L 135) 27 (EES, VIS, ETIAS, border control) [hereinafter Interoperability Regulation I]; European Parliament and Commission, Regulation (EU) 2019/818, 2109 O.J. (L135) 85 (Eurodac, law enforcement, ECRIS-TCN) [hereinafter Interoperability Regulation II].

[147] Interoperability Regulations I and II, arts. 6–11.

[148] Interoperability Regulations I and II, arts. 12–16.

[149] Interoperability Regulations I and II, arts. 17–24.

[150] Interoperability Regulations I and II, art. 20.

databases without obtaining prior authorisation by a verifying authority. In the event of a 'hit', the second step is to obtain access to each individual system that contains the matching data through the procedure prescribed for each database.[151] Finally, the MID will use the alphanumeric data stored in the CIR and the SIS II to detect multiple identities; it will create links between identical data to indicate whether the individual is lawfully registered in more than one system or whether identity fraud is suspected.[152]

III SURVEILLANCE OF MOVEMENT AND PRIVACY: A BALANCE RIGHTLY STRUCK?

1 *A Concise Typology of Standards of Privacy Protection*

The collection, storage and further processing of personal data through databases inevitably raises questions regarding the protection of the right of third-country nationals to private life, as enshrined in Article 8 European Convention on Human Rights (ECHR) and Article 7 EU Charter of Fundamental Rights (EUCFR), and personal data protection as encompassed in Article 8 EUCFR.[153] Both rights are not absolute and may be limited pursuant to Article 52(1) EUCFR, provided that the limitations to the right are provided for by law, genuinely meet an objective of general interest to the EU, safeguard the essence of the rights and respect the principle of proportionality, which entails considerations of appropriateness and strict necessity. Perhaps unsurprisingly, the proliferation of databases has not been accompanied by a substantial privacy assessment by the Court of Justice of the European Union (CJEU), presumably due to lack of awareness of or interest in the privacy issue, given the other more pressing rights at stake, such as non-refoulement.

Be that as it may, there is significant Strasbourg and Luxembourg jurisprudence on surveillance practices at the national and EU levels that contains important standards. In both Courts, the systematic collection and storage of personal data has been repeatedly found to constitute an interference with the

[151] Interoperability Regulations I and II, art. 22.

[152] Interoperability Regulations I and II, arts. 25–36.

[153] See also Article 16 TFEU. The relationship between the two rights has been the subject of extensive debate. The view taken here is that the right to personal data protection safeguards and reinforces the right to private life, rather than replaces it. As such, emphasis is placed on the standards set down in the case law of the European Courts, rather than the data protection principles that are implicitly embedded in and inform the judicial analysis. For an analysis of this thesis and a detailed typology of privacy standards see Vavoula, *Immigration and Privacy in the Law of the European Union*, chapter 1.

right to private life – or in EU terms as a limitation to the right to private life – irrespective of whether the data will be further used or the collection took place in an intrusive manner.[154] A central consideration has been whether the personal data processing 'taken as whole' allows for precise conclusions to be drawn on the private lives of the individuals affected.[155] Retention of biometric identifiers has been singled out as 'not inconsequential, irrelevant or neutral'.[156] Furthermore, the transmission of data to, and subsequent use by, other public authorities is considered a separate interference with the right to privacy since it expands the group of individuals with knowledge of the personal data.[157]

The principles of necessity and proportionality are a key requirement in the area of mass surveillance, featuring prominently in the case law of both European Courts.[158] In *Digital Rights Ireland* and *Tele2*, the Grand Chamber of the CJEU condemned generalised surveillance through the collection, retention and storage of everyday personal data – a practice which 'is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'.[159] Therefore, the CJEU found the indiscriminate collection of personal data without any differentiation, limitation or exception to be unlawful.[160] Rather, the Court held that data collection must be confined to situations that pose a threat to public security – restricted to a time period, a geographical zone, groups of persons likely to be involved in a serious crime, or more broadly persons whose communications may contribute to law enforcement.[161] In Opinion 1/15, the transfer of Passenger Name Records (PNR) data by air carriers and their subsequent use by

[154] *Amann* v. *Switzerland*, ECLI:CE:ECHR:2000:0216; *Rotaru* v. *Romania*, ECLI:CE:ECHR:2000:0504.

[155] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* v. *Ireland*, ECLI:EU:C:2014:238, para. 27; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB* v. *Post-och Telestyrelsen*, and *Secretary of State for the Home Department* v. *Tom Watson, Peter Brice, Geoffrey Lewis*, ECLI:EU:C:2016:970, para. 99; Opinion 1/15 of the Court (Grand Chamber) (26 July 2017), ECLI:EU:C:2017:592, para. 150 ('very specific information').

[156] *S and Marper* v. *UK*, ECLI:CE:ECHR:2008:1204, para. 84. Also see Case C-291/12, *Schwarz* v. *Stadt Bochum*, ECLI:EU:C:2013:670.

[157] *Weber and Saravia* v. *Germany*, 46 EHRR SE5 (2008).

[158] As I explain elsewhere, in the jurisprudence of the ECtHR, a series of privacy standards have been pronounced under the doctrinal label of legality rather than proportionality. See Vavoula, *Immigration and Privacy in the Law of the European Union*, chapter 1.

[159] *Digital Rights Ireland*, para. 37.

[160] *Digital Rights Ireland*, para. 57; *Tele2 Sverige AB*, paras. 105–108; Case C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner*, ECLI:EU:C:2015:650, para. 93.

[161] *Maximillian Schrems*, para. 93.

Canadian authorities was accepted as an appropriate instrument for the purpose of fighting terrorism and other serious crimes.[162]

As regards biometrics, in *S and Marper* v. *UK*, the ECtHR held that the retention of biometrics in connection with persons who are not suspected of a criminal offence may lead to discrimination and stigmatisation and may undermine the presumption of innocence.[163] Furthermore, in the *Schwarz* case, which concerned the storage of two fingerprints in EU biometric passports, the CJEU stressed the impact on the individual both in terms of the possibility of a false match (between the fingerprints of the passport holder and the fingerprints in the passport) and as regards the registration of fingerprint data *per se*. The Court found that storage of these fingerprints in a medium, such as the passport, is proportionate, as it remains with their owner[164] and the fingerprints are used for verification purposes.[165] A possible mismatch 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 establish their identity.[166]

Ex post access, further processing and retention periods are subject to further requirements: they must be restricted to what is strictly necessary, respect procedural and substantive conditions, and be limited to the purposes of preventing, detecting and prosecuting well-defined serious offences.[167] In *Zakharov* v. *Russia*, the ECtHR took the view that surveillance was lawful and proportionate only if based on reasonable suspicion, 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."[168] In addition, the ECtHR found that surveillance and access to data should be subject to prior review by a court or independent administrative body entrusted with ensuring compliance with constitutional and legislative limits on data processing.[169]

Moreover, retention periods should be limited on the basis of the data's potential usefulness and should remain as short as possible.[170] In Opinion 1/15

[162] Opinion 1/15 of the Court (Grand Chamber), paras. 186–189.
[163] *S and Marper*, para. 122.
[164] *Schwarz*, para. 48.
[165] *Schwarz*, para. 56.
[166] *Schwarz*, para. 43.
[167] *Digital Rights Ireland*, paras. 60–62; *Tele2 Sverige AB*, para. 115.
[168] *Zakharov* v. *Russia*, ECLI:CE:ECHR:2015:1204, para. 260.
[169] *Digital Rights Ireland*, para. 62; *Tele2 Sverige AB*, para. 120; in Opinion 1/15 of the Court (Grand Chamber) the CJEU even stated that such review is 'essential' (para. 202).
[170] *S and Marper*, para. 119; *Digital Rights Ireland*, paras. 63–64.

on the EU-Canada PNR Agreement the Grand Chamber of the CJEU distinguished between different situations: the transfer and storage of PNR data prior to (and for the purpose of) the entry into Canada; further use and storage during the passenger's stay; and the retention of PNR data after his or her departure. Whereas *storage* before entry was found to be proportionate,[171] the *use* of data during the stay had to be based on new circumstances and objective evidence.[172] Importantly, after departure, passengers subject to entry and exit checks should be regarded as 'not presenting, in principle, a risk' for terrorism and serious crime. Once a passenger leaves Canada, therefore, there is no prima facie connection – not even indirect – between their PNR data and the objective of the agreement (fighting terrorism and serious crime) that would justify retaining the data.[173] Consequently, *continued storage* of all air passengers' data after departure is not justified and only in specific cases, on the basis of objective evidence, is storage of certain passengers' data.[174]

2 *The Case of Databases for Non-EU Nationals*

The standards analysed in the previous section are applicable to the collection of personal data for immigration and border control purposes and, even more specifically, to the use of that data by law enforcement authorities. The personal data contained in the EU's immigration databases reveal very specific information about the privates lives of individuals – regarding their travel habits, their personal status, possible personal associations, in the case of the VIS, and even their educational and occupational background, in the case of the ETIAS. The following section unpacks the key privacy concerns by providing paradigmatic examples from the various databases on the issues of the necessity of specific information systems, the personal scope of such systems, the categories of personal data collected, the retention periods foreseen and the law enforcement access granted.[175]

2.1 Appropriateness Revisited: 'Mind the (Informational) Gap'

A key issue underpinning the operation of databases is whether their initial establishment and operation are appropriate for the purposes pursued.

[171] Opinion 1/15 of the Court (Grand Chamber), paras. 197–198.
[172] Opinion 1/15, paras. 199–202.
[173] Opinion 1/15, paras. 204–208.
[174] Opinion 1/15, paras. 204–208.
[175] For an in depth analysis see Vavoula, *Immigration Control and Privacy in the Law of the European Union*.

A primary example of the appropriateness issue is the operation of Eurodac as a support mechanism for an arguably ill-functioning Dublin system.[176] Although Eurodac's initial establishment was not necessarily problematic,[177] it is broadly accepted that the Dublin system is not currently 'working' for either asylum seekers or Member States. On the one hand, asylum seekers are not deterred from defying the Dublin rules and moving on to Member States in the EU core, to seek decent reception conditions and to lodge their asylum applications.[178] On the other hand, both the CJEU[179] and the ECtHR[180] have released landmark rulings condemning appalling reception conditions, leading to the halt of transfers to Greece since 2011 in view of its systemic deficiencies. The case of Greece is not the sole example. Available statistics demonstrate that during the period 2008–2012, only around 25 per cent of outgoing requests resulted in transfers, meaning that Dublin transfers take place in only around 3 per cent of all European asylum cases.[181] A Commission evaluation of the Dublin III Regulation confirms the very low number of transfers in comparison to the number of Dublin requests.[182] In light of this, the failings of Dublin have a domino effect on the operation of Eurodac, stripping away its necessity and appropriateness. 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 questioned. In the light of this, the refurbishment and reconceptualisation of Eurodac as a tool for 'wider migration purposes' is questioned and it could be argued that this tweak has been promoted in order to disentangle the system from its asylum origins and thus legitimise its existence in view of the challenges surrounding the operation of the Dublin

[176] Elspeth Guild et al., *New Approaches, Alternative Avenues and Means of Access to Asylum Procedures for Persons Seeking International Protection*, Doc. PE509.989, 2014.

[177] This pronouncement is with a caveat about the fingerprinting of irregular border crossers. See Vavoula, *Immigration Control and Privacy in the Law of the European Union*, chapter 4.

[178] On this issue, see among others, Jesuit Refugee Service, "Protection Interrupted: The Dublin Regulation's Impact on Asylum Seekers' Protection The DIASP Project," 2013, www.refworld.org/docid/51d152174.html; Susan Fratzke, "Not Adding Up: The Fading Promise of Europe's Dublin System," Migration Policy Institute, 2015.

[179] 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*, ECLI:EU:C:2011:865.

[180] *MSS* v. *Belgium and Greece*, ECLI:CE:ECHR:2011:0121; *Tarakhel* v. *Switzerland*, ECLI:CE:ECHR:2014:1104.

[181] Guild, "Moving the Borders of Europe," 9.

[182] European Commission, *Evaluation of the Implementation of Dublin III Regulation – Final Report, DG-Home* (2016), 56–57.

system. Eurodac's expansion also seems to disregard the fact that the SIS II already stores alerts on persons who must be refused entry or stay.

Furthermore, the added value of establishing the EES and the ETIAS as new databases monitoring the movement of almost all foreign travellers is not evident, particularly in light of the operation of the VIS, which was only fully rolled out worldwide in 2016.[183] Whether the EES will tackle the issue of overstayers is highly uncertain: the information mechanism envisaged does not signify that the person is necessarily an overstayer, as there may be other reasons why a person has not exited properly, e.g. human error, illness, application for asylum, death.[184] Importantly, national authorities will not have further information as regards the whereabouts of the person in question.[185] Moreover, the necessity of the ETIAS has been based on the perceived risk posed by visa-exempt travellers, without, however, substantiating the existence of that risk. The lack of an impact assessment prior to the adoption of the proposal and the pre-2015 decision to discard the project are testaments of the logic underpinning this field:[186] fill any and all 'information gaps', rather than address clear evidence-based operational needs. In this logic, necessity and appropriateness are based on data greediness, technological availability and an evolving understanding of travel as an a priori suspicious activity that legitimises the intervention of the EU as a norm creator. The new generation of databases is being created with a view to completing, through systematic personal data processing, the 'puzzle' of non-EU nationals interacting with the EU in any way, be it administrative or law enforcement.

2.2 Non-EU Nationals Concerned

The puzzle approach to databases is also evident in the personal scope of immigration databases. A key example of the EU's sweeping monitoring of the movement of third-country nationals, irrespective of proportionality considerations, is the grounds for entering alerts in the SIS II. In the first years of operation of the system, it was estimated that 77 per cent of alerts were entered

[183] Valsamis Mitsilegas, *The Criminalisation of Irregular Migration in Europe: Challenges for Human Rights and the Rule of Law* (London: Springer, 2015), 34.
[184] Ben Hayes and Mathias Vermeulen, *Borderline – The EU's New Border Surveillance Initiatives* (Berlin: Heinrich Böll Stiftung, 2012), 41.
[185] Meijers Committee, Note on the Smart Borders Proposals, CM1307, 2.
[186] See Alegre, Jeandesboz, and Vavoula, "European Travel Information and Authorisation System (ETIAS)," 27.

for the wrong reasons, raising questions of procedural fairness in SIS decision-making.[187] In a similar vein, the decision to register irregular migrants in the SIS rested entirely within the discretion of national authorities, resulting in significant discrepancies in the implementation.[188] Certain Member States, Germany and Italy in particular, were more rigorous in inserting alerts[189] and, therefore, third-country nationals faced differential treatment depending on the State in which they were found to be irregularly entering or staying. Over time, efforts to harmonise the recording of alerts stepped up, but divergences still persist.[190] In certain Member States the threshold for entering alerts is significantly higher than in others. For instance, in Lithuania, the refusal or annulment of a visa and the refusal or withdrawal of a residence permit triggers a SIS II alert, whereas in other Member States the categories set out in the Regulation are followed.[191] In numerous States an expulsion decision (return) is automatically accompanied by an alert.[192] The mandatory registration of entry bans and return decisions in the refurbished SIS II will signify a further watering down of the SIS II standards and will lead to automatic storage of personal data of essentially all irregular migrants irrespective of how serious the violation of immigration law. By inclusion of this data, registration in the SIS II becomes unavoidable, even in cases when the individual has voluntarily left the national territory, which is disproportionate in view of the personal conduct of the person concerned. The proportionality criterion for the registration of alerts is thus nullified, substituted by race-to-the-bottom harmonisation.

The expansive approach to personal scope, this time explicitly linked to security concerns, is also illustrated by the proposal to expand the VIS to include holders of residence permits, residence cards and long-stay visas. In the VIS reform, the inability to verify the identity and documentation of these categories of persons against a centralised system is framed as a potential

[187] Stephen Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Cooperation* (Leiden: Martinus Nijhoff, 2008), 216.

[188] Brouwer, *Digital Borders and Real Rights*, 61–62.

[189] Schengen Joint Supervisory Authority, Article 96 Inspection – *Report of the Schengen Supervisory Authority on the Inspection of the Use of Article 96 Alerts in the Schengen Information System* (20 June 2005).

[190] For an analysis see Vavoula, *Immigration and Privacy in the Law of the European Union*, chapter 2.

[191] European Migration Network, "Ad Hoc Query on Procedures for Entering Foreigner's Data into the Schengen Information System," 2014, http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/border/505_emn_ahq_procedures_entering_foreigners_data_into_the_sis__7jan2014_%wider_dissemination%29.pdf.

[192] European Migration Network, "Ad Hoc Query on Procedures for Entering Foreigner's Data."

'threat to the security of one of the Member States'.[193] In other words, in an era of 'Security Union', security and migration are fully intertwined and a permanent cloud of suspicion surrounds not only individuals who may have undergone a series of checks for obtaining legal documentation but also the Member States who granted the residence status, who can only trust each other if an EU technological fix intervenes. In addition, from the perspective of the allocation of competences, it is questionable whether the VIS, as a Schengen *acquis* instrument, may be expanded to include categories of nationals whose documentation is not regulated by EU rules, but remains a competence of the Member States.

2.3 Categories of Collected Information

The categories of personal data collected, stored and further processed within databases merits some attention, as the high volume of personal data collected in certain cases goes beyond necessity and proportionality. For example, in the VIS, a category of personal data that raises proportionality concerns is that of persons issuing an invitation or sponsoring the stay of a visa applicant, persons who may be EU citizens or third-country long-term residents. In the course of routine implementation of the EU visa policy, the processing of these data is excessive and disproportionate and may lead to the creation of a mini-register on the side. Furthermore, in light of law enforcement access to the VIS data, their registration and consultation raises further concerns, as their data may be used in police investigations. Another example of disproportionate collection comes from the ETIAS and the processing of data on the applicant's level of education; the US ESTA does not collect this category of information and it is not clear why the ETIAS needs to do so.

Furthermore, the routine storage of biometrics – a special category of personal data – in all databases but the ETIAS is questionable. In contrast with the storage of fingerprints in biometric passports, at issue in the *Schwarz* case, in databases biometrics are stored centrally and therefore the individuals concerned lose control of their personal data. Furthermore, when biometrics are centrally stored, the error rates are impacted by the number of persons contained in the system.[194] Therefore, the larger the system, the greater the probability of a 'hit' based on an error. In cases of large-scale databases holding millions of records, the possibility of a false match is enhanced,

[193] *Commission Proposal*, COM (2018) 302 final.
[194] Kindt, *Privacy and Data Protection Issues of Biometric Identifiers*, 59.

particularly if there are data quality issues.[195] Such an error can have severe consequences: the wrongful return of the individual to another Member State on the basis of a Eurodac hit; refusal of entry into the Schengen area; or even implication of the person in criminal proceedings in the framework of law enforcement. In addition, a full set of fingerprints is arguably disproportionate for immigration control purposes and can only reasonably be justified if their use is limited to criminal law purposes. Indeed, given that the VIS – and the revised Eurodac, if agreed – includes a digital photo, the collection of fewer fingerprints would have sufficed for identification purposes, even though that would frustrate the ancillary purpose of the systems to assist in crime prevention or investigation.

2.4 Retention Periods

The period during which personal data must be retained is vital, as continued storage and use of data perpetuates the effects of the interference with the right to private life. In the case of Eurodac, the ten-year retention period for asylum seekers was never properly justified; even though the Parliament had suggested reducing it to five years, the amendment was ignored by the Council.[196] As for the current eighteen-month retention period for the fingerprints of irregular border crossers, it does not correspond to the one-year responsibility of Member States for asylum seekers under Dublin rules. Furthermore, in the case of the SIS II, broad leeway has been granted to Member States: the three-year rule for deletion of the data subject to review without any maximum retention period being imposed on the Member States. The current trend points to an emerging default retention period of five years (SIS II,[197] VIS,[198] Eurodac,[199] EES,[200] ETIAS[201]). Among other things, this default for all EU databases appears to be useful for the purposes of interoperability.

Importantly, in light of the CJEU Opinion 1/15 on the EU-Canada PNR agreement, the EU's existing and proposed databases make no distinction between the different phases of a non-EU national's journey. For example,

[195] For data quality issues of the VIS in particular, see Vavoula, *Immigration and Privacy in the Law of the European Union*, chapter 3.
[196] Aus, "Eurodac: A Solution Looking for a Problem?"
[197] SIS II Proposal, art. 34.
[198] Excluding visa holders whose data are kept for ten years. See VIS Regulation, art. 23.
[199] See *Commission Proposal*, COM (2016) 272 final, art. 17(2) and (3).
[200] In the case of potential overstayers, see EES Regulation, art. 34(3).
[201] In cases of refusal, annulment, revocation of the travel document. See ETIAS Regulation, art. 54.

both the EES and the ETIAS – the latter as a result of Member State pressure – will continue to store personal data even after the departure of the individual concerned in order to serve immigration-control purposes. However, according to the CJEU case law, after the departure of travellers, storage is justified only in relation to certain individuals on the basis of objective evidence. Therefore, the premise of databases as systems which may encompass an array of purposes creates a paradox, whereby the continued storage of personal data of all individuals captured by the database may be justified for administrative purposes, but has a significant spillover effect because of law enforcement access to their data, and perpetuates the risk for the individuals concerned.

2.5 Law Enforcement Access

There are also a number of issues related to law enforcement access to databases for non-EU nationals. As explained earlier, in the case of the SIS II, the interrelation between immigration control and law enforcement was pre-embedded in the structure of the system, which had no unitary and limited purpose. Even though its main preoccupation was and continues to be immigration control, a *de facto* mission creep into law enforcement has thus been evident. Furthermore, the ECRIS-TCN is a law enforcement tool aimed at enabling Member States to exchange criminal records on non-EU nationals. With regard to the remaining databases, law enforcement access is an ancillary purpose – an add-on to the overarching functions of the system and as such, for the time being, such consultation may take place under specific circumstances only. Nevertheless, it must be stressed that law enforcement access is not obvious[202] and compelling evidence justifying the addition of this purpose must be adduced. As with the necessity of setting up the databases in the first place, justification of the need for law enforcement access has often been fragile.[203] Furthermore, the Eurodac example clearly illustrates the inherent danger of mission creep when personal data is centrally stored: once information is stored for a specific purpose, there is a real possibility of the system being re-purposed for objectives that were not initially contemplated.

[202] As is demonstrated by the fact that in designing the EES, the Commission initially left out law enforcement, and a proposal for recasting the Eurodac Regulation, including law enforcement access to asylum seekers' data, was blocked by the European Parliament in 2009.

[203] For the case of Eurodac see Niovi Vavoula, "The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?" in *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System*, eds. Céline Bauloz et al. (Leiden: Brill, 2015), 260.

As for the modalities of law enforcement access, these substantially fall short of the standards set out by the European Courts. Whereas the conditions are indeed set out and no routine access is foreseen in the individual legal instruments, a series of loopholes remain. The national authorities allowed to consult the data are those responsible for the prevention, detection and investigation of terrorist offences or of other serious criminal offences as designated at the national level.[204] As is evident from this expansive definition, national governments have considerable leeway to designate a wide array of agencies.[205] There is no other guidance, requirement or limit contained in the EU legal instruments. Indeed, national intelligence agencies may also be given access if the Member State so chooses; only in the case of Eurodac have intelligence services been explicitly excluded.[206] The inclusion of intelligence services is worrisome; although it is to be welcomed that they are bound by the same rules as the rest of national authorities,[207] their operation is obscure when compared to police agencies. Once a Member State determines which authorities are to be given law enforcement access, the list of designated authorities is communicated to the Commission and published in the Official Journal, but there is no EU-level control and oversight. Finally, with regard to the procedure for consulting the data, in all cases, the designated authorities must submit a reasoned electronic request to an authority (Central Access Point or in the case of Eurodac to a Verifying Authority) that ascertains that the conditions for obtaining access have been met. Nevertheless, this procedure is not in line with the criteria set out in *Digital Rights Ireland*, *Tele2*, and Opinion 1/15, where the CJEU explicitly required that law enforcement access to the data be made dependent on prior review carried out by a court or by an independent administrative body. Considering that requesting and verifying authorities may be part of the same law enforcement agency, the independence and objective judgment of the necessity of access may be jeopardised.

2.6 (Not so Innocent) Interoperability

With the adoption of the new Regulations on interoperability, the landscape of information processing through centralised databases will be forever

[204] The list of competent authorities is published in the Official Journal, but may differ significantly both across the different databases and among Member States.
[205] Mitsilegas, "Human Rights, Terrorism and the Quest for 'Border Security'," 109.
[206] Eurodac Regulation, art. 5(1).
[207] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council Concerning the Visa Information System (VIS) and the Exchange of Data between Member States on Short-Stay Visas (COM(2004)835 final), 2005 O.J. (C 181) 13.

changed. Whereas it has been correctly pointed out that interoperability will not frustrate existing limits on *access* rights of national authorities, it must be highlighted that the *use* of personal data will be attached to new purposes, which are not to be found in the respective legal instruments. For instance, in the interoperability legislation, Eurodac data will be used to detect persons with multiple identities even though Eurodac's mandate does not specify this use. Another worrisome change involves the possibility for a Member State *police* authority to query the CIR with the biometric data of a person taken during an identity check, solely for the purpose of identifying that person.[208] This function of the CIR is not supported by the existing legal framework and current EU law, aside from the Interoperability Regulations, does not spell out the circumstances and conditions under which their identity checks shall take place.[209] Overall, interoperability further downplays the importance of the purpose limitation principle and 'disrespects the importance of separated domains and cuts through their protective walls'.[210]

Importantly, the operationalisation of interoperability involves the masked setting up of new databases based on combining data from different sources – the BMS, the CIR and the MID.[211] The fancy wording that is used ('component' and 'repository') should not distract from the dangerous reality of massive catalogues of third-country nationals at EU level.[212] The aggregation of data through databases signifies a new information-processing paradigm of mass and indiscriminate surveillance. By combining information from different systems, brand new systems emerge, authorities are empowered to draw more precise conclusions on the private lives of individuals, and data subjects are unable to foresee how their collected information will be used. It is not far-fetched to characterise interoperability as a decisive step away from a compartmentalised system of independent databases and towards a single EU information system in the service of an EU Big Brother.

Another key change brought about by interoperability involves law enforcement access to non-EU nationals' data. Although, as mentioned previously, access is currently reserved for specific cases based on the necessity of consulting the data, interoperability marks a significant step towards routine access.

[208] Interoperability Regulations I and II, art. 20.

[209] Tony Bunyan, "The Point of No Return – Interoperability Morphs into the Creation of a Big Brother Centralised EU State Database Including All Existing and Future Justice and Home Affairs Databases," Statewatch, May 2018, 10.

[210] De Hert and Gutwirth, "Interoperability of Police Databases within the EU," 27.

[211] Presumably the MID will not store personal data *per se*, but confirmation files that contain the links between alphanumeric data related to identity stored in the CIR and the SIS.

[212] Opinion 4/2018 of the European Data Protection Supervisor (16 April 2018), 11.

The regulations stipulate a two-step approach, in which designated authorities shall first check all systems through the CIR on a hit/no hit basis and then, if they get a hit, satisfy the conditions applicable to each of the underlying databases to obtain access to the individual data pots.[213] Yet even just a hit is significant since it reveals elements of an individual's personal life, for instance that they are visa free travellers, and therefore the first step of checking whether there is personal data should be covered by the conditions of access. Importantly, it is hard to believe that upon finding that a database holds information on a person, the verifying authority ensuring the conditions for access have been met will not allow such access. In other words, not only the independence and objectivity but also the very existence of a verifying authority may be biased by the two-step approach.

IV CONCLUSION

The aim of this chapter has been twofold: to map the evolution of pan-European databases for non-EU nationals and to highlight a series of privacy concerns that have been triggered by their establishment, operation and reconfiguration over time. Through the systematic categorisation of EU information systems in three distinct eras, it has been demonstrated that their operation entails the collection and storage of a wide range of personal data, including biometrics, and their further processing for multiple and often diverging purposes, which are anything but fixed. In the future, driven by the logic of closing information gaps, lack of EU citizenship will entitle State authorities to require individuals to provide extensive personal data, including sensitive data. The big picture is that of systematic expansion of the personal scope of EU databases: once the aforementioned systems are fully operational, no non-EU citizen will be left un-surveyed through at least one database. Apart from expanding the groups of individuals concerned and the purposes and the categories of data to be collected, the initial compartmentalised approach has been abandoned in favour of interoperability, enabling the data pots to interact. The aggregation of data will not only generate new databases and new data (MID) but will also transform existing databases – particularly those originally created for administrative, immigration control purposes – into powerful intelligence tools.

[213] See Teresa Quintel, "Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention," University of Luxembourg Law Working Papers, March 2018, 16.

These trends have utterly blurred the boundaries between immigration and criminal law.[214] They had been driven by, and will in turn feed, the perception of non-EU nationals as potential risks for EU internal security, and have significant repercussions for their privacy. This chapter had provided concrete examples of disproportionate data processing by scrutinising the operating rules of the many databases, as well as their interoperability, against the jurisprudential benchmark of the European Courts. The necessity and appropriateness of information systems has been taken for granted rather than robustly justified; the existence of the old generation of databases has generated a domino effect, in which their operational flaws are used to unreflexively justify the new and revised systems. Furthermore, specific categories of information should not be available to certain authorities. With the routine registration of biometrics, the provision of extensive retention periods and the use of data for law enforcement purposes, the administration of non-EU nationals through electronic databases has progressively been transformed into a system of mass surveillance of movement. Particularly in the VIS, the EES and the ETIAS, everyday legitimate activities are monitored.[215] Travel has emerged as an inherently dangerous activity and mobility operates as a trigger for state surveillance.

With surveillance of movement becoming the norm, a key question remains: will it expand to cover EU nationals, undermining not only their privacy but also EU citizenship rights? This is more than a rhetorical question. As explained earlier, with respect to both the EES and the ECRIS-TCN, it was suggested that EU nationals also be included. These examples seem to tentatively confirm the dystopian predictions, raised in the introduction, that the new technologies are being tested on foreigners so that they can then be extended to EU nationals. In light of the comprehensive coverage of non-EU nationals, it appears that the trial period has come to an end. Indeed, in an era when every non-EU national is potentially a risk justifying security surveillance, the divide between the privacy safeguards for EU and non-EU nationals will become acute. Might, in the future, the standards of privacy protection for EU nationals be lowered to close this gap? It remains to be seen what the future will bring to the ongoing battle between security and privacy. It is only hoped that the outcome has not already been decided.

[214] For further exploration of this theme, see Chapter 11.

[215] See David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001).