The ability of computers to recognise faces, fingerprints, irises, DNA sequences, human language and other body-related aspects, has provided us with a powerful tool to verify an individual's identity, and thus to ensure the maintenance of a certain level of security. Biometric technology is no longer in an embryonic development stage. Instead, it is found at the heart of national and international security and immigration policies. The use of biometrics is not without risk, however. Biometric technology incorporated in machine-readable documents allows for enhanced surveillance. In addition, the theft of biometric data, unique by nature, might be far more detrimental for the person concerned than the loss of other personal data.

Part I
Overview of legal instruments

1. Eurodac

Eurodac explained
Eurodac is a computerised, central database set up to assist in determining which EU Member State is responsible for examining an asylum application lodged in a Member State. Eurodac has been established by Council Regulation (EC) 2725/2000 of 11 December 2000, which covers the establishment of a system “Eurodac” for the comparison of fingerprints, thus facilitating the effective implementation of the Dublin Convention3.

The Dublin Convention4 aims to avoid the ‘orbiting’ of asylum seekers by preventing asylum applications in different Member States. The convention has been replaced by the Council Regulation 343/2003 (Dublin II Regulation) of 18 February 2003. Generally speaking, someone seeking asylum is required to lodge an application in the Member State where he/she first arrived. In principal, personal data included in Eurodac may be processed only for the purposes set out in the European human rights framework. The scope of these frameworks will be briefly explained and linked to the provisions set out in the Regulations. The third section takes a more critical look at the Eurodac Regulations, and the draft Regulation for VIS and the European Passport (regulations that rely on the body as a ‘document’ or a ‘tool’ for the purposes of identification). The third and final section will also cover (i) the choice in favour of biometrics as a means of identification and verification, (ii) the legal framework underlying the laws establishing Eurodac, the VIS, and European Passports and travel documents, (iii) the validity of the Eurodac, VIS and European Passport in light of the principles of proportionality, finality and individual participation, and (iv) the issue of a central biometric database. The second and third section will be published in a future edition of the journal.
Article 15 (4) of the Dublin Convention, which stipulated that “Each Member State shall communicate to any Member State that so requests such information on individual cases as is necessary for: - determining the Member State which is responsible for examining the application for asylum, - examining the application for asylum, - implementing any obligation arising under this Convention.”

The Eurodac system consists of a Central Unit that operates the central database and means of transmission between the Member States. The unit is established within the Commission. There are three categories of people (or data subjects), whose data are processed in Eurodac: (i) applicants for asylum (asylum seekers), (ii) aliens apprehended in connection with the irregular crossing of an external border, and (iii) illegal aliens in a given Member State. The biometric data consists of fingerprints. Given the specific purpose of the Dublin Convention, the processing objectives and data retention periods are separately specified and regulated for each of these categories.

**Asylum seekers**
Each Member State is required to fingerprint (all fingers of) every asylum seeker aged 14 or over. The fingerprint data is subsequently submitted to the Central Unit, alongside details of the applicant’s gender and other pertinent application data. The Central Unit will record the data in the central database. Once entered by the Central Unit, the applicant’s fingerprints are compared to fingerprints already stored in the database (these were previously submitted by the Member States). The comparison covers only previously recorded fingerprints of asylum seekers and aliens apprehended while illegally crossing an external border. Fingerprints taken from illegal aliens encountered in a given Member State are not recorded in Eurodac.

The comparison will either be positive or negative. If a match is found, all data corresponding to the hit will be transmitted to the Member State that submitted the data for comparison. The Member State in question will check the comparison before a final identification is made in cooperation with the Member States.

**Aliens apprehended while illegally crossing external borders**
Each Member State is required to fingerprint (all fingers of) every alien aged 14 and over who is apprehended by the competent control authorities while illegally crossing the border of a Member State, said alien having come from a third country and not having been turned back. The Member State subsequently submits the fingerprint data to the Central Unit, alongside details of the alien’s gender and other relevant fingerprint data. The Central Unit will record the data in the central database.

The personal data of aliens apprehended while illegally crossing an external border will be recorded for the sole purpose of comparison with data relating to asylum seekers that is received by the Central Unit after the alien’s personal data has been received. In other words, the biometrics of aliens who have been apprehended will not, on arrival at the Central Unit, be compared to previously-stored data. Instead, these fingerprints will be used at a later stage to identify future asylum seekers.

**Aliens found illegally staying in a Member State**
Unlike the fingerprints of asylum seekers and aliens apprehended while illegally crossing an external border, which must be taken immediately, the authorities are under no immediate obligation to take the fingerprints of aliens who illegally stay in a given Member State. Instead, Member States may transmit the data to the Central Unit any fingerprint data that it may have obtained from any such alien aged 14 or over. Similarly, while the fingerprints of asylum seekers and aliens caught while illegally crossing an external border must be recorded in the central database, no such obligation exists in relation to aliens who illegally stay in a given EU Member State. Fingerprint data may only be transmitted to the Central Unit with a view to checking whether the illegal alien has previously applied for asylum in another Member State. Therefore, the fingerprint of the illegal alien may only be compared to fingerprint data of asylum seekers who have already been recorded in the central database. This data may not be compared to previously recorded fingerprint data of aliens apprehended while illegally crossing an external border.

**Purpose of the database and access rights**
The Member States’ right to access data in the central database are limited. Moreover, the task of comparing fingerprints falls to the Central Unit. Member States can only transmit data for specific purposes (see supra) and are only given access to data if the Central Unit has encountered a hit following a “lawful” comparison. Member States always have access to all data that they have submitted to the Central Unit themselves. However, they may never conduct a search against data submitted by other Member States.

**Data retention periods for the central database**
Data relating to asylum seekers are stored for a period of ten years from the date on which the fingerprints were taken. The data will be deleted earlier if the applicant has acquired citizenship of a Member State. Data relating to recognised and legal refugees (in a given Member State) will be blocked until such time as the Eurodac Regulation is amended by other regulations. Until that time, the Central Unit will return hits in relation to recognised and legal refugees as negative results.
Data relating to aliens apprehended while illegally crossing an external border will be stored in the central database for two years from the date on which the fingerprints were taken. This data will be deleted earlier if the alien has obtained a residence permit, left the Member States in question or acquired EU citizenship\(^5\). Data relating to illegal aliens are not stored, and will only be used for comparison purposes (data is deleted once the results of comparison have been returned).

**Data controllers and responsibilities**\(^22\)

The Member States are responsible for (i) legally obtaining fingerprints (the Member States act as data controllers in this regard), (ii) the lawful transmission of accurate and up-to-date personal data to the Central Unit, (iii) the lawful use of the results of the fingerprint comparison, (iv) the final identification of the data subject on receipt of the results of the fingerprint comparison, and (v) the confidentiality and security of the national installations as well as the data (before, during and after the transmission thereof).

The Commission (the Central Unit) is responsible for the lawful recording, storage, correction and deletion of data in the central database. It is also responsible for the confidentiality and security of the Central Unit and the central database.

**The rights of the data subjects**

The rights of the data subjects, which are elaborated in the European Data Protection Directive 95/46 (see infra), apply. The data subjects must be informed of (i) the identity of the controller and its representative, (ii) the reasons why the data is processed within Eurodac, (iii) the recipients of the data released by Eurodac, (iv) the obligatory nature of fingerprinting (except for aliens who are illegally present in a Member State - supra) and (v) the right to access and rectify incorrect data\(^21\). The data subjects’ rights include the right to an explanation by the controller of the logic of the processing involved, at least if ‘automated decision taking’\(^22\) takes place, and the right to request that ‘factually’ inaccurate or unlawfully-recorded data be corrected or erased by the Member State that transmitted the data\(^23\).

**The future of Eurodac**

On 24 November 2005, the Commission sent a Communication to the Council and the European Parliament to improve the effectiveness and interoperability of - and among - European databases\(^24\). As far as Eurodac is concerned, the Commission concluded that the database has been under-exploited given that the quantity of the data transmitted to Eurodac is a ‘surprisingly low fraction of the total migratory flow’\(^25\). It also noted that (i) too much data would increase the likelihood of incorrect results and wrong identification, and (ii) many illegal immigrants have no valid ID document, making the identification process time-consuming and expensive. On the other hand, the Commission concludes that the Member States have no means of checking whether an asylum seeker has had a (valid) visa issued. Moreover, the inability of internal security authorities to access Eurodac data is ‘considered by the law enforcement community to be a serious gap in the identification of suspected perpetrators of a serious crime’.

In view of the above, the Commission defines ‘further possible developments’ for Eurodac and, among others, lists more comprehensive access to Eurodac by authorities responsible for internal security in well-defined cases (‘when there is a substantiated suspicion that the perpetrator of a serious crime has applied for asylum’).

**2. The European Visa Information System (VIS)**

**Explanation**

On 28 December 2004, the Commission proposed a Regulation\(^26\) calling for the establishment of (a legal framework for) a European Visa Information System (VIS), to be used for the exchange of data relating to short-stay visas between Member States. The establishment of the VIS greatly helps the European Union to achieve a common policy on the exchange of visa data between Member States. It also allows the EU to guarantee the free movement of persons and abolish checks at internal borders\(^27\). This would prevent people from filing several visa applications in different Member States, and allow visa authorities to check the visa history of a given individual. The VIS Proposal also includes other finalities that enable different authorities to access the system for purposes other than visa policies\(^28\). The VIS consists of a central database that falls under the responsibility of the Commission (CS-VIS). It is connected to the different national interfaces (that fall under the responsibility) of the Member States (NI-VIS).

**Photographs and fingerprints in a central database**

The individuals (or data subjects) whose information is stored in the database are third country nationals who have filed a visa application. Citizens from 134 countries require a visa to enter the EU\(^29\). All requisite application data will be processed in the central VIS database.

The personal data processed comprises alphanumeric information relating to the applicant as well as his or her photograph and fingerprint (biometric data\(^30\)). The personal data, which are entered in the system as soon as the application for a visa is submitted, are linked to other visa applications (think, for example, of applications by members of the same travelling group.
or previous applications by the same applicant). The application file stored in the VIS database will contain other personal information such as the grounds for refusal, annulment, revocation or extension of the visa. The biometric data will be stored in a centralised database (VIS). For the time being, the biometric data will not be stored on the visa sticker (uniform format for visas) that accompanies the valid travel document as this may cause technical conflicts as a result of too many biometric identifiers being included in a single document for example, a travel document containing a passport identifier as well as visa identifiers in relation to visas issued by other countries. In other words, the documents of the visa holders do not contain biometrics.

**Purpose of the database and access rights**

The right to access, amend or delete data in the VIS is only extended to duly authorised staff employed by the visa authorities. The right to access and consult data in the VIS is in the first place extended to duly authorised staff employed by visa authorities to examine applications, to consult and request documents, to report, and to generate statistics. Data stored in the VIS may also be consulted by duly authorised staff of other authorities provided they are competent for activities beyond a common visa policy. Inherently, they access the VIS for different reasons. In view of the above, the following authorities are permitted to access at least (i) the alphanumerical data referred to in article 6(4)(a) and (ii) the biometrics (photograph and fingerprints) of the applicant.

1. Competent authorities - carrying out checks on visas at external borders and within the territory of the Member State for the sole purpose of verifying the identity of the person and/or the authenticity of the visa (Article 16).

2. Competent immigration authorities - solely for the identification and return of illegal immigrants (Article 17).

3. Competent asylum authorities - solely in order to determine the Member State responsible for examining an asylum application and to examine an asylum application (articles 18 & 19).

In other words, VIS may be accessed to examine applications, to improve the administration of the common visa policy, and to facilitate consular cooperation, all with the aim of (i) preventing threats to internal security and ‘visa’ shopping, (ii) facilitating the fight against fraud, (iii) assisting in the identification and return of illegal immigrants and (iv) facilitating the application of the Dublin II Regulation. The Commission will table a proposal allowing Europol as well as internal security authorities to access VIS for clearly defined purposes. As early as 2005, the Council decided to allow law enforcement authorities to access VIS in the future.

**Data retention periods for the central database**

The data retention period for each application file is maximised at five years, starting on the last expiry date of the visa or the date on which the application file was created in VIS if no visa is issued. The application file will be deleted earlier if (i) the data appear to be inaccurate, (ii) the data in the VIS are not processed in accordance with the Regulation or (iii) the applicant has acquired the nationality of a given Member State.

**Data controllers and responsibilities**

In their capacity as data controllers, the Member States are responsible for (i) the lawful processing of data, (ii) the lawful collection and transmission of data to the VIS (in an accurate and up-to-date format) and (iii) data confidentiality and security before and during transmission to NI-VIS and following receipt from VIS. In addition to the confidentiality and security of the CE-VIS, the Commission is responsible for the communication infrastructure between CE-VIS and NI-VIS.

**The rights of the data subjects**

The visa applicants have the right to be informed by the responsible data controller of the controller’s identity, the purpose of processing within the VIS, the recipients of the data, the mandatory nature of the data collection and the right to access and amend or delete data.

**The future of the Visa Information System**

In the aforementioned Commission Communication, the inability of internal security authorities to access the VIS is considered a serious obstacle to the identification of suspected perpetrators of a serious crime. The intelligence communities also considered the fact that VIS only deals with third country nationals to be a shortcoming. (The control of the identity or
the legality of the entry of other categories of third-country nationals (…) eg, holders of a long-stay visa or a residence permit (…) could also be more efficient’). Finally, the fact that VIS cannot be used to identify illegal aliens in the EU is considered ‘incomplete monitoring of entry and exit of third country nationals’44. As far as VIS is concerned, the Communication calls for the ‘further development of existing systems and planned systems’ in the following areas: (i) expanding the ability of asylum and immigration authorities to access the system, (ii) extending access to authorities responsible for internal security for the purposes of preventing, detecting and investigating terrorist offences and (iii) allowing the system to be used to identify victims of (natural) disasters and unidentified bodies45.

To conclude, the Commission also stated that ‘the development of a service-oriented architecture of European IT systems would help maximise synergies’ thus providing ‘a way of sharing functions in a flexible and cost-efficient way without merging existing systems’. The Commission even gives an example: “In concrete terms, one example would be to use the highly performing future AFIS part of the VIS to deliver AFIS-related services (ie, a biometric search for other applications, such as EURODAC or, possibly, a biometric passport register). Data storage and data flows could still be strictly separated46.”

3. The European passport

**Explanation**

Although some Member States already issue biometric passports, the EU is initiating far-reaching changes as far as biometric passports and travel documents for EU citizens are concerned. Having introduced minimum security requirements for EU passports and travel documents in 200047, the European Union has meanwhile upgraded, standardised and harmonised the minimum security features, and included biometric requirements for passports and travel documents in Council Regulation 2252/200448.

The minimum level of security applicable to passports and travel documents issued by Member States is laid down in the Annex to the Regulation and relates to the specific materials used, the machine-readable biographical data page, the printing techniques, protection against copying and issuing techniques. As far as standards for biometric features are concerned, Regulation 2252/2004 states that these must comply with the standards laid down by the International Civil Aviation Organization (ICAO) in ICAO Document 930349.

The biometrics for passports and travel documents were introduced by virtue of this Regulation ‘in order to render the travel document more secure and to establish a more reliable link between the holder, the passport and the travel document’50. At first sight, the use of biometrics therefore looks to verify the validity of a claimed identity instead of establishing a person’s identity51. The main provisions of Council Regulation 2252/2004 are listed below.

**Facial image and fingerprints stored on a RFID chip**

Passports and travel documents issued by the Member States must include a storage medium that contains a facial image. Member States shall also include fingerprints in interoperable formats52. The Regulation expressly states that no machine-readable information shall be included in the passport or travel document unless foreseen in the Regulation or specifically mentioned in the passport or travel document by the issuing Member State53. The storage medium, which must have sufficient capacity and capability to guarantee data integrity, authenticity and confidentiality, is a RFID chip. This was decided by the Commission in February 200554.

Whether the biometric data - captured when the passport or travel document is applied for and stored in the passport or travel document - are also stored in a central database is not covered in Regulation 2252/2004, despite being an important issue. Consequently, it is up to the Member States to decide whether they wish to import the biometrics in a central database. In other words, there is no special provision imposing or forbidding the storage of passport biometrics in a central database.

**Box 1**

**Comparison with Eurodac and VIS**

Unlike Eurodac and VIS, biometric passports and travel documents are physical documents assigned to people. People with a biometric passport carry the biometrics with them. Eurodac and VIS are databases - identification and verification does not take place on the basis of documents.
**Purpose of the biometric features**

The biometric features in passports and travel documents shall, for the purpose of the Council Regulation, only be used to verify the authenticity of the document and the identity of the holder. Verification takes place on the basis of directly available comparable features whenever the passport holder is required to produce his or her passport by law.

**The rights of the data subjects**

Persons to whom a passport or travel document is issued will - without prejudice to data protection rules - have the right to (i) verify the personal data contained in the passport or travel document and (ii) ask for data to be rectified or deleted, where appropriate.

**Limited scope and implementation**

Council Regulation 2252/2004 does not apply to national identity cards or temporary passports and travel documents having a validity of 12 months or less. Moreover, the scope of harmonisation is limited to the security features that include biometric identifiers. The designation of authority to access data in the document’s storage medium remains a matter of national legislation.

Member States must include digital facial image and fingerprints in their passports by 28 August 2006 and 28 February 2008 respectively.

The fact that EC Regulation 2252/2004 does not address the issue of a central database (this has been left to the Member States) can have a significant impact in terms of privacy and data protection. The (disputable) safeguards that have been defined in relation to VIS and Eurodac (access rights, responsibilities, confidentiality and security, and the rights of data subjects) have not been stipulated for EU passports.

**Future of the passport**

There is some indication - at EU level - that a centralised national database for EU passport and travel documents is in the pipeline. For example, in February 2006, the Dutch government repeated its intentions to develop a central database for passports and previously-issued travel documents, which database should include biometric data. Although the Commission’s Communication notes that ‘there is no comprehensive database which would allow for the identification of disaster victims and unidentified bodies’, this appears to be a somewhat far-fetched justification for the introduction of interconnected and interoperable EU passport databases.

The intention to interlink national DNA databases highlights a desire among authorities to combat crime and terrorism with the support of an umbrella network of interlinked databases.

Finally, the Commission’s Communication points out that ‘most Member States will have a central repository of issued documents and biometric identifiers linked to a certain identity’ even if ‘a query of that central repository only allows a check as to whether in that same Member State a document has been previously issued to the same person under another name. In addition, it is currently not possible to launch a query on a person who is, say, wanted for a terrorist crime on the basis of whether this person has ever been issued with a travel or ID document’. The Commission even concludes that this ‘gap in the fight against identity theft (...) substantially damages the European economy.

In a subsequent edition of this journal we will discuss the European human rights framework and apply its basic principles to the EU regulatory framework governing machine-readable identity documents featuring biometric data. Although all EU laws consistently refer to the human rights framework as a necessary starting point, it will become clear that this starting point is not always respected, at least in our view.
1 Part of this contribution borrows from our work within the Fidis network. This network is funded by the 6th Community Framework Programme in Research and Development (FP 6). See on FIDIS (the Future of Identity in Information Society) www.fidis.net.


4 Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities - Dublin Convention, Official Journal C 254, 19 August 1997, 1-12.

5 Although Eurodac is not considered as a travel document (there is no travel document or passport or visa issued) and although Eurodac does not contain other data than the fingerprints and the sex of the fingerprint owners, the fingerprints of these people are used for identification and verification purposes (see infra).

6 An ‘applicant for asylum’ is defined as ‘an alien who has made an application for asylum or on whose behalf such an application has been made’ (Article 2.1.a of the Eurodac Regulation).

7 Besides fingerprint data and sex, the following data are transmitted to the Central Unit and recorded in the central database: Member State of origin, place and date of the application for asylum; reference number used by the Member State of origin; date on which the fingerprints were taken and on which they were transmitted to the Central Unit. The Central Unit adds the date on which the data were entered in the central database and details in respect of recipient(s) of data transmitted and the date(s) of transmission(s) (See Article 5).

8 Article 4 of the Eurodac Regulation. The Central Unit can use these data for statistical purposes (see Article 3 of the Regulation).

9 Article 4 of the Eurodac Regulation describes the procedure.
10 See footnote 6.
11 Article 4.5: ‘...although in the case of [fingerprint data], only insofar as they were the basis for the hit’. This extension makes it unclear whether only fingerprints or also other data are used to compare.
12 Article 4.6 of the Eurodac Regulation.
13 Article 8 of the Eurodac Regulation. Article 1 of the Dublin Convention defines an alien as ‘any person other than a national of a Member State’.
14 Besides fingerprint data and sex, the following data are transmitted to the Central Unit and recorded in the central database: Member State of origin, place and date of apprehension; reference number used by the Member State of origin; date on which the fingerprints were taken and on which they were transmitted to the Central Unit. The Central Unit adds the date on which the data were entered in the central database and details in respect of recipient(s) of data transmitted and the date(s) of transmission(s) (See Article 5).

15 Article 11 of the Eurodac Regulation.
16 Article 15 of the Eurodac Regulation.
17 Article 6 and 7 of the Eurodac Regulation.
18 The amendment can take place after a period of five years after the Eurodac implementation. This amendment will provide whether data concerning recognised and admitted refugees will be stored for 10 years from the date when the fingerprint has been taken, or be erased in advance (Article 12.2).
19 Article 10 of the Eurodac Regulation.
20 Article 13 and 14 of the Eurodac Regulation.
21 This information shall be given to asylum seekers and aliens apprehended in connection with the irregular crossing of external borders ‘when the fingerprints are taken’ Aliens found illegally will receive this information ‘no later than the time when the data relating to the person are transmitted to the Central Unit’, unless ‘the provision of such information proves impossible or would involve a disproportionate effort’.
22 Article 15 of the Data Protection Directive: “1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. 2. (…) a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision: (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject’s legitimate interests.
23 Article 18 of the Eurodac Regulation.
27 Article 29 Data Protection Working Party, ‘Opinion on the

28 See also infra. Article 1.2 of the VIS Proposal summarizes the different purposes, namely to: (a) prevent threats to internal security of any of the Member States; (b) prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application; (c) facilitate the fight against fraud; (d) facilitate checks at external borders and within the territory of Member States; (e) assist in identification and return of illegal immigrants; (f) facilitate application of EU Regulation 343/2003.


30 Article 3.1. Article 6 lists the alphanumerical data that are entered in the application file. Some of the alphanumerical data are surname, first names, sex, date, place and country of birth, nationality, type of travel document, place and date of application, application number and the visa status information.


33 Visa authorities are defined as authorities of each Member State which are responsible for examining applications and for decisions taken hereto of for decisions whether to annul, revoke or extend visas (Article 2 (3)).

34 Article 13, 14 and 15 of the VIS Proposal.

35 Surname, surname at birth (earlier surname(s)); first names, sex, date, place and country of birth.

36 Article 2 (10) of the VIS Proposal defines verification as “the process of comparison of sets of data to establish the validity of a claimed identity (one-to-one check)”. Article 2 (11) of the VIS Proposal defines identification as “the process of determining a person’s identity through a database search against multiple sets of data (one-to-many check)”. Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs, Brussels, 24.11.2005, COM(2005) 597 final, 4.

39 Conclusions meeting Council of 7 March 2005, doc. 6811/05, of 40 Article 21 and 22.