SCRIPT-ed

Volume 4, Issue 3, September 2007

The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards

Dr. Gerrit Hornung*

Abstract

The current implementation of biometric data in the new generation of European passports is progressing rapidly. On the legal basis of an EU Council regulation, member states must include RFID chips containing facial and fingerprint images in the travel documents of their citizens. While the use of biometric systems itself poses fundamental questions of constitutional and data protection law, the political and legislative procedures implemented prior to the adoption of the Regulation have been highly problematic due to the absence of public debate, the lack of participation of the national parliaments and the overruling of the European Parliament by the Council. Furthermore, important practical issues remain unsolved.

DOI: 10.2966/scrip.040307.246

---

* Dr. Gerrit Hornung, LL.M. in European Law (Edinburgh), Managing Director, Projektgruppe verfassungsverträgliche Technikgestaltung (provet), University of Kassel, gerrit.hornung@uni-kassel.de. An earlier version of this paper was presented at the Workshop 'Privacy and Information: Modes of Regulation' (A Busch and C D Raab), ECPR Joint Session of Workshops, Helsinki, 7-11 May 2007.

1. Background

On December 13, 2004, the EU Council passed the Regulation on standards for security features and biometrics in passports and travel documents issued by the member states.[1] According to Article 6, the States have to include biometric facial images in their passports 18 months, at the latest, after the establishment of technical standards, which took place in February 2005.[2] For fingerprints, the time frame is 36 months, *i.e.* the deadline is February 2008. Some states, including Germany, started to issue the first version of the new passports (RFID chip with facial data) at the end of 2005.

Although (most)[3] member states are directly bound by the Regulation, there remains the need for national provisions, particularly concerning the issuance procedures and the authority to read and match the data. Moreover, essential questions (*e.g.* the problem of nation-wide databases) have not been addressed by the Regulation and thus left to the member states. In early 2007, the German government introduced a bill for the amendment of the National Passport Act (*Passgesetz*), which was passed by the Bundestag on 24 Mai 2007.[4] Similar legislation is underway in other member states.

---

[1] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal 2004 L 385, 1; see A Roßnagel and G Hornung, "Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck. Die EG-Verordnung 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten", *Die Öffentliche Verwaltung* 2005, 983 ff. (hereafter referred to as Roßnagel and Hornung, "Reisepässe").

[2] These standards are not publicly available in their entirety. However, there is a Decision of the Commission establishing the technical specifications on the standards for security features and biometrics in European passports, which includes the public parts of those standards, see European Commission, Decision establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States, C(2006) 2909 of 28/06/2006, available in German at http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_de.pdf (there is no English version, since the UK and Ireland have not taken part in the adoption of this measure; the standards are available in English at http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_prov_en.pdf).

[3] The UK and Ireland did not take part in the adoption of the Regulation and are not bound by it, because it constitutes a development of provisions of the Schengen Acquis in which the UK (in accordance with Council Decision 2000/365/EC of 29 May 2000) and Ireland (in accordance with Council Decision 2002/192/EG of 28 February 2002) do not take part. Nevertheless, the new British and Irish passports will comply with the European requirements; see UK National Audit Office, "Introduction of ePassports. Report by the Comptroller and Auditor General", HC 152 Session 2006-2007, 7 February 2007, available at http://www.nao.org.uk/pn/06-07/0607152.htm, 8 (hereafter referred to as UK National Audit Office, "Introduction of ePassports").

[4] See G Hornung, "Fingerabdrücke statt Doktortitel: Paradigmenwechsel im Passrecht. Der Gesetzesentwurf der Bundesregierung zur Änderung des Passgesetzes und weiterer Vorschriften", *Datenschutz und Datensicherheit* 2007, 181 ff. (hereafter referred to as Hornung, "Fingerabdrücke")

This development poses highly controversial legal, political and technical questions, which are further aggravated by the split between the European and the national legal provisions. Some of the main legal issues include the questions of nation-wide databases, the purpose the biometric data is put to, back-up procedures and the use of RFID-chips. At the same time, the new passports are a characteristic example of the conflicts which have arisen between privacy and new surveillance measures since the attacks of September 11 2001, regarding the attitude of the respective players, the political and legislative process and the (absence of any real) public debate before the definite decision had been made. The last issue is closely related to the question of legitimacy of the particular surveillance measures. In what follows, the aforementioned topics will be addressed with particular emphasis on the legal situation in Germany.

2. Biometrics, RFID and Privacy

Biometrics is the automated means of recognising a living person through the measurement of distinguishing, physiological and behavioural traits.[5] Fingerprint systems are the most widely used and reached a market share of one third in 2003.[6] Face, iris, hand geometry, voice and handwriting are among the other most common biometrics.

Regardless of the respective biometric, the systems operate in similar ways.[7] First, users' reference data is captured and stored (enrolment). The percentage of persons which are not successfully enrolled into the system is referred to as false enrolment rate or failure to enrol rate (FER). Such problems may be due to system failure. Nonetheless, for almost every biometric, there is a certain percentage of people who either do not possess the respective feature (due to accidents or disability) or whose biometrics do not entail enough distinguishing characteristics. While it is possible to use facial recognition with almost everybody, the FER is estimated to be 1 to 4 per cent (finger) and 1 per cent (Iris), respectively.[8] Furthermore, the use of the system can also be momentarily hampered by physical injuries.

---

[5] See *e.g.* J D Woodward, Jr, N M Orlans and P T Higgins, *Biometrics. Identity Assurance in the Information Age*, (2003), 7 (hereafter referred to as Woodward, Orlans and Higgins, *Biometrics*); A Albrecht, *Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz* (2003), 31 (hereafter referred to as Albrecht, *Biometrische Verfahren*); M Behrens and R Roth, *Biometrische Identifikationssysteme: Auf dem Weg vom Labor zum Markt. Eine Bestandsaufnahme – unter Berücksichtigung der USA* (2001), 1 f. (hereafter referred to as Behrens and Roth, *Biometrische Identifikationssysteme*); G Hornung, *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren* (2005), 75 (hereafter referred to as Hornung, *Die digitale Identität*).

[6] Woodward, Orlans and Higgins, *Biometrics*, 213.

[7] See in detail Albrecht, *Biometrische Verfahren*, 35 ff.; Behrens and Roth, *Biometrische Identifikationssysteme*, 10 ff.; Hornung, *Die digitale Identität*, 78 ff.; G Hornung, "Biometrische Systeme - Rechtfragen eines Identifikationsmittels der Zukunft", *Kritische Justiz* 2004, 346 ff. (hereafter referred to as Hornung, "Biometrische Systeme"); Woodward, Orlans and Higgins, *Biometrics*, 28 ff. Some technical particularities (such as template-free systems) are of no significance for the passports.

[8] Woodward, Orlans and Higgins, *Biometrics*, 22, 99.

The reference data may be stored completely (image data) or in the form of extracted features (template data). In the authentication procedure (matching), these images or templates are compared with the newly captured biometrics. This can be done in two different ways. If the reference data is stored in a central database (or a network of linked local databases), the new data is sent to a central system and matched against the whole database (identification, 1:n matching). The other possibility is local storage in movable devices, such as a biometric passport (verification, 1:1 matching). In these cases, the data is either matched in the device (matching-on-card) or in the reader.

Due to measuring errors, unsuitable biometrics and other inaccuracies, there is never a definite result of the matching. Thus, the possibility of false rejection or false acceptance always remains. The percentages of matching errors are described as false rejection rates (FRR) and false acceptance rates (FAR), respectively. Both rates depend on the accuracy of the system and on the threshold which has to be met for a positive match. The higher this threshold is set, the lower the FAR will be. A high threshold may be desirable for instance in high security areas, but at the same time poses the problem of a higher FRR and authorised persons may be at risk of becoming suspect or even being permanently rejected. However, while a low threshold provides convenience, it causes the FAR to rise and thus poses security risks. Therefore, both failure rates depend on each other and the optimal system configuration can only be identified in relation to the specific operating conditions.

While the use of biometrics allows for the preservation of personal privacy (*e.g.* when used to control the access to personal IT systems),[9] biometric passports are clearly an example of how security and privacy interests come into conflict. There is some dispute about the question of in which circumstances biometric data constitutes "personal data" as defined in Art. 2 a) of the EU Data Protection Directive[10] and national legislation.[11] Additionally, the meaning of "personal data" in the respective national legislation may differ. While the German *Bundesdatenschutzgesetz* (federal data protection act) takes a rather broad approach, the UK Court of Appeal held in *Durant* v *Financial Services Authority*[12] that 'personal data' is only "information that affects [a person's] privacy, whether in his personal or family life, business or professional capacity". Nonetheless, the biometric data in an identity document is in any case personal data, as it is inseparably linked to the name which is printed on the surface of the document, and affects the privacy of the holder.

In the specific case of European passports, facial and fingerprint images are to be stored on RFID chips, which are passive, *i.e.* they carry no source of power, but

---

[9] J D Woodward, "Biometrics: Identifying Law and Policy Concerns", in A Jain, R Bolle and S Pankanti (eds), *Biometrics. Personal Identification in Networked Society* (1999), 385; Hornung, *Die digitale Identität*, 85 f.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 31.

[11] For the German discussion, see G Hornung, "Der Personenbezug biometrischer Daten", *Datenschutz und Datensicherheit* 2004, 429 ff. (also available at http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/DuD%202004,%20429%20Hornung.pdf)

[12] Durant v Financial Services Authority [2003] EWCA Civ 1746.

instead derive power indirectly from the reader signal. The intended read range is set to about ten centimetres.

A decision was made against the use of templates to prevent interoperability problems. This decision is problematic because image data contains more information about the data subjects. In certain cases this includes health data. There are indications that it is possible to infer certain diseases from fingerprint data (*e.g.* breast cancer, Rubella syndrome, and certain chromosomal disorders such as Down's syndrome, Turner syndrome, and Klinefelter syndrome).[13] Scientific medical research suggests that iris data could be connected to diabetes, arteriosclerosis und hypertension,[14] HIV and misuse of alcohol and drugs,[15] or even homosexuality.[16] While the latter might be speculative, any sole suspicion could lead to disadvantages for the person affected.

In addition to the fact that biometric data can be sensitive in itself, the use of such data evokes further risks for the data subject. Central databases may be used to control great parts of public behaviour. Even though face recognition does not yet work with large databases (with more than approximately 10,000 records), this could change in the future and allow for imperceptible individual surveillance measures. The possibility to capture data through contactless interfaces (RFID chips) causes conflicts with one of the most important safeguards of data protection law, the principle of transparency.[17] Fingerprints are involuntarily left on everyday objects, which makes it feasible to trace individual moves and actions over a long time.[18] Importantly, the life-long inseparable connection to a person facilitates data collection and profiling, and may even hamper the lawful change of an identity within witness-protection programmes.

As for legal safeguards, it is unclear from its wording whether the EU Data Protection Directive applies to biometric passports and identity cards.[19] However, in Recital 8 of

---

[13] Woodward, Orlans and Higgins, *Biometrics*, 202 f.

[14] Woodward, Orlans and Higgins, *Biometrics*, 203.

[15] Albrecht, *Biometrische Verfahren*, 173.

[16] J A Y Hall and D Kimura, "Dermatoglyphic Asymmetric and Sexual Orientation in Men", *Behavioral Neuroscience* 108 (1994), 1203 ff.; S LeVay, *Queer Science: the Use and Abuse of Research into Homosexuality* (1996), 157 f.

[17] G Hornung, "Biometric Identity Cards: Technical, Legal, and Policy Issues", in S Paulus, N Pohlmann and H Reimer, H. (eds), *ISSE 2004: Securing Electronic Business Processes* (2004), 53 (also available at http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/Hornung_Buch_ISSE_2004.pdf) (hereafter referred to as Hornung, "Biometric Identity Cards"); on the issue of transparency and biometric smartcards see also G Hornung, "Datenschutz für Chipkarten. Die Anwendung des § 6c BDSG auf Signatur- und Biometriekarten", *Datenschutz und Datensicherheit* 2004, 15 ff. (also available at http://www.uni-kassel.de/fb7/oeff_recht/publikationen/ pubOrdner/DuD-2004-15.pdf).

[18] On a similar DNA problem, see D H Kaye, "Science Fiction and Shed DNA", *Northwestern University Law Review* 2006, available at http://www.law.northwestern.edu/lawreview/colloquy/2006/7/.

[19] Pursuant to Art. 3 (2) and recital 13, the Directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of EC law, such as those provided for by Titles V (provisions on a common foreign and security policy) and VI (provisions on police and judicial cooperation in criminal matters) of the Treaty on European Union and in any case to processing operations concerning public security, defence, state security and the activities of the state in areas of criminal law.

the European Regulation on Biometric Passports, it is stated that "with regard to the personal data to be processed in the context of passports and travel documents", the Directive applies.

In any case, States must comply with Art. 8 ECHR and their respective constitutional privacy provisions. There is a considerable amount of concurrence among national data protection requirements: interferences authorised by the state can only take place on the basis of law specifying in detail the required circumstances; the processing of the data must be proportional in relation to the interference; the intended use of the data must be specified before it is collected, and the subsequent use is restricted to those purposes; unless there are express legal provisions, data can only be collected with the knowledge or consent of the data subject (principle of transparency); the data subject possesses certain rights against the data controller; appropriate security measures have to be taken for the protection of personal data against inadvertent or unauthorised destruction, or accidental loss, as well as against unauthorised access, alteration or dissemination.

In a number of publications, these principles have been applied to biometric passports. According to the authors, this leads to the following, general, requirements:[20]

- The biometric identifier must be suitable for the purpose of a general identity document, *i.e.*, the secure 1:1 verification of a large group of cardholders. Thus, the biometric has to be universal, while the system must operate with low failure rates: FAR and FRR should be less than 1 %.[21]
- According to the principle of proportionality, preferred biometrics do not include additional information, are not permanently left in one's environment, and require the cooperation of the card holder.[22] However, these criteria do not conclusively lead to one biometric feature.
- Generally speaking, the use of templates is preferable from the viewpoint of data protection law.[23] Yet, in the specific case of international travel documents, this is, in part, held back by the lack of template standardisation.

---

[20] See, e.g. C Golembiewski and T Probst, *Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen*, available at http://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf, 2003 (hereafter referred to as Golembiewski and Probst, *Datenschutzrechtliche Anforderungen*); Büro für Technikfolgenabschätzung beim Deutschen Bundestag, *Biometrie und Ausweisdokumente. Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zweiter Sachstandsbericht*; available at http://www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf, 2003; (hereafter referred to as Büro für Technikfolgenabschätzung, *Biometrie und Ausweisdokumente*); H Reichl, A Roßnagel and G Müller, *Der Digitale Personalausweis* (2005) (hereafter referred to as Reichl, Roßnagel and Müller, *Personalausweis*); Roßnagel and Hornung, "Reisepässe", 983 ff.; Hornung, *Die digitale Identität*; G Hornung, "Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues", *European Public Law* 2005, 506 ff. (hereafter referred to as Hornung, "Biometric Passports"); L Meuth, *Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen* (2006); some of the following requirements are highly controversial.

[21] Reichl, Roßnagel and Müller, *Personalausweis*, 121 f.

[22] See in detail Hornung, *Die digitale Identität*, 178 ff.; Reichl, Roßnagel and Müller, *Personalausweis*, 123 f.

[23] Albrecht, *Biometrische Verfahren*, 158; Hornung, "Biometric Identity Cards", 53; see also Reichl, Roßnagel and Müller, *Personalausweis*, 231 f.; Hornung, *Die digitale Identität*, 78 f., 188 ff.

Therefore, the International Civil Aviation Organisation (ICAO) opted, very early on, for the use of image data. It should also be stressed that the storing of biometric templates still requires the use of raw data for each matching. This significantly reduces the advantages for the data subject.

- To ensure data security on the chip, there must be strong encryption, authentication, and electronic signature processes in place, particularly in the case of sensitive data.[24]
- The misuse of data must be prevented on a technical level by enrolment and matching devices.
- States must install back-up procedures to both ensure the secure identification of all persons, and to avoid discrimination of those either unable to enrol in the system or temporarily unable to use it (see below 4.3.).
- Central, as well as local, databases are not necessary for passport control procedures as the data is to be matched against the reference data on the chip. Whether or not central databases can be justified on the grounds that they prevent citizens from obtaining several identity documents with different names or on grounds of general crime prevention needs depends largely on national constitutional requirements (see below 4.1).[25]

As mentioned earlier, the last question is left completely to the member states. Thus, even though the European Regulation provides for a basic interoperable European passport system, the actual interference with the human rights of the respective citizens will vary to a considerable extent. So far, no comparative research has been carried out in this respect.

3. The EU Council Regulation on Biometric Passports

3.1. Content[26]

According to Art. 1 (3), Regulation (EC) Nr. 2252/2004 applies to passports and travel documents issued by the member states. Notably, it does not apply to identity cards, because those cards do not fall within the ambit of the European competences.[27]

Pursuant to Art. 1 (2). "Passports and travel documents shall include a storage medium which shall contain a facial image. Member states shall also include fingerprints in interoperable formats." The latter formulation relates to the lack of

---

[24] Hornung, *Die digitale Identität*, 198 f. with further references.

[25] Even if answered affirmatively, this would still raise the question of whether or not those databases are necessary to achieve this aim.

[26] The following section focuses on the issue of biometrics. The Regulation also entails other provisions, such as minimum security standards, technical specifications and conditions for bodies having responsibility for printing passports and travel documents; see Roßnagel and Hornung, "Reisepässe", 984 ff.

[27] Art. III-125 (2) of the Treaty establishing a Constitution for Europe (Official Journal C 310 of 16.12.2004, 1 ff) contains such a competence, but it remains unclear if and when the treaty will enter into force.

template standardisation and has led to the plan to store fingerprint images. Art. 1 (2) also includes the requirement that "the data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data". This wording should not be misunderstood as only describing the technical capabilities of the RFID chip. Instead, the provision entails a binding obligation to actually secure the data in the described way.[28] This is possible through the use of public-key infrastructures (PKI), which allow for electronic signatures (integrity and authenticity), mutual authentication procedures and encryption (confidentiality) (see below 4.4.).

Art. 4 of the Regulation comprises specific data protection provisions. According to Art. 4 (1), "persons to whom a passport or travel document is issued shall have the right to verify the personal data contained in the passport [...] and, where appropriate, to ask for rectification or erasure". As it is impossible for the holder to verify the data herself/himself (due to the electronic storage and encryption), passport authorities (or specific government agencies) are obliged to provide suitable RFID readers at local places. Art. 4 (2) states that "no information in machine-readable form shall be included in a passport or travel document unless provided for in this Regulation, or its Annex, or unless it is mentioned in the passport or travel document by the issuing Member State in accordance with its national legislation".

The purposes of the biometric features are specified in Art. 4 (3) of the Regulation, which reads as follows: "For the purpose of this Regulation, the biometric features in passports and travel documents shall only be used for verifying (a) the authenticity of the document; (b) the identity of the holder". Note however that while the intended use of biometric information seems to be severely limited, the wording of the Regulation leaves open the possibility that nation states legislate for the use of this data for other purposes as well.

Eventually, the verifying process may only be carried out "by means of directly available comparable features when the passport [... is] required to be produced by law". This complies with the principle of transparency and bars the use of passport data without the knowledge of the data subject.

3.2. Players and Legislative Procedure

The EU member states are but a large group among the countries which are currently implementing biometric passports. Generally, the USA is seen as the dominant player in this development. Sec. 303 (c) of the Enhanced Border Security and Visa Entry Reform Act originally stipulated that "not later than October 26, 2004, the government of each country that is designated to participate in the visa waiver program [...] shall certify, as a condition for designation or continuation of that designation, that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with applicable biometric and document identifying standards established by the International Civil Aviation Organization". Although this deadline was extended twice by one year, it put significant pressure on the governments of the visa waiver countries. At the same time, those governments were, to a considerable

[28] Roßnagel and Hornung, "Reisepässe", 985.

extent, relieved from the duty of having to justify the new passports as they were able to claim that they were only following international demands (see also below 5.).

This factor was enhanced even more by the fact that the ICAO came up with several standardisation documents.[29] Despite the lack of any explicit authorisation in the treaty on which the organisation is based (the Convention on International Civil Aviation, or "Chicago Convention"),[30] it has claimed responsibility for the standardisation of travel documents for more than 50 years.[31] As almost all states have committed themselves to act in accordance with the ICAO documents (particularly DOC 9303 on Machine Readable Travel Documents and the technical reports on biometrics deployment, the use of PKI and contactless ICs and the development of a logical data structure), the ICAO has become one of the most influential actors in this area.

At the same time, it is not to be forgotten that the organisation is in no way democratically controlled. While every Member State has the right to vote in the Assembly, the ICAO Council is comprised of 33 members, which are elected in a way that gives "adequate representation to (1) the States of chief importance in air transport; (2) the States not otherwise included which make the largest contribution to the provision of facilities for international civil air navigation; and (3) the States not otherwise included whose designation will insure that all the major geographic areas of the world are represented on the Council" (Art. 50 (b) Chicago Convention). Furthermore, the standardisation activities depend largely on human and financial resources provided by the members. Thus, those willing to offer this support may gain substantial influence in this respect.

While the standards and recommendations of the ICAO are not legally binding as such, the EU Council Regulation on Biometric Passports of 13 December 2004 states that the member states shall comply with them in regard to passports. Through this mechanism, the ICAO requirements concerning RFID chips and facial images became mandatory for all EU members except the UK and Ireland.[32] It should be stressed however that the use of fingerprint data is required neither by ICAO nor by US demands and therefore is solely based on the decision of the EU Council.

The European institutions hold quite different views on the opportunities and risks of biometric systems. In a 2005 report, the Commission drew a very optimistic picture of future commercial applications in almost all areas of life.[33] In contrast, there are critical statements from the European Data Protection Supervisor and the Article 29 Data Protection Working Party.[34]

---

[29] See Hornung, "Biometric Passports", 504 f.; standardisation activities are primarily conducted by the ISO/IEC JTC 1 SC 37 and 17.

[30] Available at http://www.icao.int/icaonet/dcs/7300.html.

[31] On the ICAO, see H Schäffer, *Der Schutz des zivilen Luftverkehrs vor Terrorismus: Der Beitrag der International Civil Aviation Organization (ICAO)* (2007).

[32] See note above.

[33] European Commission, *Biometrics at the Frontiers: Assessing the Impact on Society*, Report of the Joint Research Centre (DG JRC), Institute for Prospective Technological, available at ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf, 2005.

[34] Article 29 Data Protection Working Party, *Working Paper 80: Working document on biometrics, 12168/02/EN*, available at

In the course of the legislative procedure of the EU Passport Regulation, the European Parliament firmly opposed the storage of fingerprint data.[35] In the first proposal of the Commission,[36] the mandatory part was restricted to facial images, leaving the issue of fingerprints to the discretion of each Member State. In contrast to the version finally adopted by the Commission, this proposal included neither the requirement to secure the confidentiality of the data nor the lawful purposes now stated in Art. 4 (3). In both respects, the Parliament successfully demanded changes.[37]

However, the Parliament's intervention failed in regard to the ban on a European passport database, the involvement of the Art. 29 Data Protection Working Party in the standardisation process, and the use of fingerprints. According to Art. 67 (1) TEC, the Council was allowed to pass the Regulation unanimously on the proposal from the Commission, after having consulted the European Parliament. This procedure was duly carried out, although, apparently, the Parliament was put under considerable time pressure by the Council.[38] Remarkably, even the draft Regulation that was laid before the Parliament did not yet contain the provisions making the use of fingerprints compulsory. In a highly questionable move, these provisions were inserted after the fact into the text, once again without the Parliament having been consulted.

It appears that prior to adoption in the Council, none of the parliaments of the member states had approved the new passports. In Germany, the issue was debated in several hearings,[39] yet no decision was taken by the *Bundestag*, which, in an earlier Act, had even expressively reserved for itself the right to decide on the issue.[40] Statements of the national data protection supervisory authorities[41] were mainly discussed after the decision in the Council had been made.

---

http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf, 2003; and *Working Paper 112: Opinion on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 1710/05/EN*, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_en.pdf, 2005; the Working Party is composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

[35] See the legislative resolution of 2.12.2004, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2004-0073+0+DOC+XML+V0//EN.

[36] COM 2004(116), Official Journal C 98 of 23.4.2004, 39.

[37] See the legislative resolution of 2.12.2004, note 33 above.

[38] See *e.g.* http://www.heise.de/newsticker/meldung/53830.

[39] See the *Bundestagsdrucksache* No. 15/3145, 9; 15/3642, 12 ff.; 15/3663, 3; 15/3765, 4 f.; 15/4211, 7 ff.; 15/4477, 8 f., 17 ff).

[40] Sec. 4 (4) National Passport Act (*Passgesetz*), see Hornung, *Die digitale Identität*, 173 ff.; Hornung, "Biometrische Systeme", 355 ff.

[41] Konferenz der Datenschutzbeauftragten des Bundes und der Länder, "Positionspapier zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen", *Datenschutz und Datensicherheit* 2002, 247 ff.

4. Main Remaining Problems

Since the adoption of the European Regulation, member states have been concerned with both its practical implementation and the remaining need for supplementary legislative measures in the national legal systems. Additionally, further problems may appear in the course of the implementation process or when the system comes into operation.

4.1. Nation-wide Databases

Concerning the storage of the data (left to the member states by the Regulation), several countries worldwide use central, nationwide biometric databases or, as in the UK, plan to do so in the future. The aim is to prevent citizens from establishing more than one identity by obtaining several passports with different names, particularly in those states which do not possess a general register of residents or are introducing it at the same time as the new identity documents.

By contrast, the German legislative had ruled out the possibility of a nationwide database in Sec. 4 (4) *Passgesetz* in 2002. Furthermore, the constitutional requirements in Germany are stricter than in most other countries. That is to say a general central biometric database (and decentralised equivalents) would be incompatible with the "*Recht auf informationelle Selbstbestimmung*" (right to informational self-determination) which forms part of the fundamental rights of the German *Grundgesetz*.[42] Moreover, there seems to be less of a necessity for a database, given the highly developed system of residents registers.

In addition, the current amendment of the National Passport Act also excludes the local storage of biometric fingerprint data in the databases of passport authorities. Subsequent to the production of the passport, the manufacturer and passport authorities are obliged to delete the data. Furthermore, this also applies after every verification process. Apart from the short-term processing of the data in specific control situations, the fingerprints are thus only to be stored in the German passport itself and not in any databases of public authorities.

Through this, the German government and parliament have resisted the temptation to use the introduction of the new passports as a means of establishing a highly problematic biometric database.[43] Given the possibility of connecting decentralised databases (in Germany, the aim to electronically connect all local municipalities was accomplished by the end of 2006), the decentralised storing of the data does not form any real safeguard. Instead, the only effective way to protect the data appears to be the

---

[42] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, *Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen*. Stand Juli 2003, available at http://www.datenschutzzentrum.de/download/ Biometrie_Gutachten_Print.pdf; Hornung, "Biometric Passports", 509; Hornung, *Die digitale Identität*, 191 ff.; Reichl, Roßnagel and Müller, *Personalausweis*, 136 ff.

[43] On the problem of such databases, see Albrecht, *Biometrische Verfahren*, 159 ff., 162 f.; Golembiewski and Probst, *Datenschutzrechtliche Anforderungen*, 69 ff.; Hornung, *Die digitale Identität*, 191 ff.; Hornung, "Biometrische Systeme", 352 f.; Woodward, Orlans and Higgins, *Biometrics*, 40.

restriction to the passports, pursuant to the principle of data minimisation. Thus, the German approach can be seen favourably.

4.2. Purpose of the Biometric Data

As mentioned earlier, the use of biometric features is limited by the European Regulation, but only "for the purpose of this Regulation" (see above 3.1.). Hence, the important question is raised which additional purposes the member states deem appropriate, and as to whether those purposes meet the respective constitutional requirements.

In Germany, no further purposes beyond those specified in the Regulation for the passport data are foreseen by the National Passport Act.[44] There are authorisations for the respective police, customs, passport and registration authorities, but the new Sec. 16a of the Act clearly states that the use of the biometric data shall be absolutely restricted to the verification of the authenticity of the document and the identity of the holder. Other authorities, as well as private actors, are strictly barred from using the biometric data.

Regarding the data stored in local databases, police authorities may, as before, access facial data to prosecute criminal offenders. However, the new Act allows for the retrieval of the electronic data, thereby significantly reducing the burden on the respective authorities and most likely increasing the numbers of retrieval requests. As the *Passgesetz* expressly outlaws a central database, it is not permitted to search the data for a specific face (*e.g.* from a CCTV camera). Additionally, it appears to be technically impossible in the medium term to identify a face within a biometric database of 70 million records with reasonable failure rates.

Since fingerprints are not to be stored in any databases, no data protection issue is raised in this respect.

4.3. Back-up Procedures

Every biometric system has to face the problem that for various reasons, a certain percentage of the population will permanently or temporarily be unable to present the biometric feature. Additionally, most of the cases of non-recognition will be false rejections (see above 2.). Even relatively low FRRs will involve high absolute numbers of such false rejections: At Frankfurt Airport, a system with an FRR of 1 % would produce more than 1,000 false alarms per day.[45]

It is currently unclear how many people will actually be confronted with these problems.[46] Yet, it is apparent that states will have to install back-up procedures to both ensure the secure identification of all persons, and to avoid discrimination of those unable to enrol in the system.[47] As the principle of equal treatment forms part of

---

[44] See in detail Hornung, "Fingerabdrücke", 182 f.

[45] Hornung, *Die digitale Identität*, 179.

[46] See in detail Hornung, *Die digitale Identität*, 179 ff.

[47] Hornung, *Die digitale Identität*, 199 ff.; J-H Hoepman, E Hubbers, B Jacobs, M Oostdijk and R W Schreuer, *Crossing Borders: Security and Privacy Issues of the European e-Passport*, available at

all constitutional systems, as well as the law of the European Union and the European Convention on Human Rights (Art. 14), this applies to all member states. Therefore, it will not be possible to rely on biometric identification alone at checkpoints. Additionally, back-up procedures must be effective to prevent delays.

Whether or not this requirement produces significant problems for border controls will only become apparent once the passport system is in regular operation, because the actual consequences for the holders depend on the further process (permission of further attempts to be recognised, in-depth control procedures, etc.). This also applies to those passport holders whose fingerprints are just barely suitable for biometric recognition. These persons may suffer additional difficulties, because they could be confronted with significantly higher individual false rejection rates than the average user.[48] To prevent such disadvantages, it would be helpful for the control person to have access to officially confirmed information concerning such problems. Sec. 4 (3) of the German *Passgesetz* adopts this course and explicitly provides for the storage of information on the quality of the biometric data in the passport chip.

In any case, the body of the ID card needs to be forgery-safe and usable without a chip, because its content could be destroyed without the owner's knowledge. At the same time, it is highly problematic to allow for the "conventional" use of passports with destroyed chips, as this might make it possible to bypass biometric controls, thereby bringing the whole project into question (see below 4.5.).

4.4. RFID – the Problems of Authentication and Encryption

While the use of contactless chips has durability advantages, data stored on such chips poses transparency problems for the card holder, who is hardly able to notice whether data is being read from the card (a problem know as "skimming").[49] Furthermore, it might be possible to record the electronic communication between the chip and the reader ("eavesdropping"). There is also the problem of misuse in cases of loss or theft.

In the beginning, the ICAO did not envisage any security measures (such as authentication and/or encryption). That would have left the holders with last resorts, such as keeping the passport in a metal jacket (*e.g.* aluminium foil) which would prevent the radio frequency reader from being able to read the data.[50] Instead, Art. 1 (2) of the EU Passport Regulation forces the member states to implement measures to guarantee the integrity, the authenticity and the confidentiality of the data (see above 3.1.), and ICAO standards now provide for optional security measures.

---

http://www.cs.ru.nl/~jhh/publications/passport.pdf, 2006, 3 (hereafter referred to as Hoepman et al., *Crossing Borders*).

[48] See Hornung, *Die digitale Identität*, 202 f.

[49] In the context of biometric documents, see Hornung, *Die digitale Identität*, 197 f.; from a technical perspective A Juels, D Molnar and D Wagner, *Security and Privacy Issues in E-Passports*, available at http://eprint.iacr.org/2005/095.pdf, 2005, 2 ff. (hereafter referred to as Juels, Molnar and Wagner, *Security and Privacy Issues*).

[50] Given the high-tech nature of biometric systems, such safeguards may seem somewhat ludicrous in the first place – yet they could prove to be the most efficient tools to protect the sensitive data.

To fulfil this duty, the first generation of biometric passports uses a so-called "basic access control" system (BAC).[51] The electronic data (biometric features and other personal information) is encrypted with an individual key, which depends on the characters of the machine-readable zone (MRZ) of the passport. At checkpoints, this information must be read first in order to unlock the chip for reading. Thus, control persons must scan the printed lines of data in order to be able to read the data on the chip. The security of BAC is, nonetheless, highly debated.[52]

As the MRZ characters are available to everybody who is in possession of the passport, the BAC system protects neither in the case of loss or theft nor against anyone who lawfully or unlawfully obtains the MRZ data. For this reason, the second generation of passports (containing fingerprint data) will be equipped with an "extended access control" system (EAC), which is based on the automatic mutual recognition between the chip and the reader.[53] In this public-key infrastructure (PKI), each country will set up a Country Verifying Certification Authority (CVCA), whose certificates are to be stored on the passport chips of that country. The CVCA will issue certificates to Document Verifiers in other countries, who in turn will administer certificates of their respective card readers. This system allows the restriction of data transfers from the passport chip to readers which are equipped with certificates that can be traced back to the CVCA of the issuing state. Accordingly, every country may decide which other countries are allowed to access the data. The EAC scheme will attenuate the data protection problems of biometric passports, however there are remaining difficulties, such as the issue of stolen card readers equipped with valid certificates and the problem that the chip cannot keep time itself and does not have access to a reliable source of time either, thus making it hard to check whether a certificate of a card reader has expired.[54]

4.5. Important Practical Problems

It is apparent that the new passports may face practical problems which could undermine the effects of the whole project. First of all, biometrics can be an effective measure of securely connecting a travel document to a person, but knowing who a person is does not necessarily provide any knowledge about this person's intention. The September 11 (2001) attacks may have been the starting point of the development of biometric passports, yet the justification they provide is weakened by the fact that at least nine of the terrorists on that day were travelling with their own (and valid) passports and had not committed any identity frauds.[55]

Moreover, the enrolment process could prevail as the weak point. If false data is inserted into this process through corruption or extortion, false identities will be

---

[51] See Juels, Molnar and Wagner, *Security and Privacy Issues*, 8 ff.; Hoepman et al., *Crossing Borders*, 4; D Kügler and I Naumann, "Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen", *Datenschutz und Datensicherheit* 2007, 178 (hereafter referred to as Kügler and Naumann, "Reisepass"); UK National Audit Office, "Introduction of ePassports", 24 f.

[52] See Hoepman et al., *Crossing Borders*, 5 ff.

[53] See Hoepman et al., *Crossing Borders*, 8 ff.; Kügler and Naumann, "Reisepass", 178 f.

[54] Hoepman et al., *Crossing Borders*, 9 f.

[55] A Towler, "Mistaken Identity?", *Law Society Gazette* 2004, No. 17, 20.

established. Usually, it will be impossible for control persons to detect this. In contrast, the identity fraud may even be harder to discover, due to the "officially approved" biometric data.

Last but not least, the issue of defective passport chips could cause major problems. First of all, the question arises as to whether or not the holder will have to bear the costs of a new passport. While this has usually been the case so far, it will be hard to justify if governments are using technology without sufficient guarantees. According to the UK National Audit Office, the "ability" of UK passports "to withstand normal usage for the full ten-year passport lifespan remains unproven".[56] Therefore, "chip units are guaranteed for only two years, leaving Identity and Passport Service vulnerable to returns".[57]

Secondly, a defective passport may provoke cases of government liability if a holder suffers damages (*e.g.* due to delays). Thirdly, a particular security problem will arise if the defect is invisible. The German *Bundesregierung* announced that in this case, the passport remains valid and the owner will be subject to the previous passport control procedure.[58] Likewise, the US Department of State declares in its website's frequently asked questions that "the chip in the passport is just one of the many security features of the new passport. If the chip fails, the passport remains a valid travel document until its expiration date".[59] As it is impossible for the owner to verify if the chip is properly functioning, this appears to be the only way to handle this difficulty. However, it may put the whole project under scrutiny if potential offenders were able to bypass the biometric control due to the invisible destruction of the RFID chip.

4.6. Financial and Acceptance Issues

It is currently difficult to estimate the total cost for a national system of biometric passports (particularly if it includes fingerprint data), partly due to the policy of nondisclosure of the European governments.[60] As regards ID cards, a UK Home Department's Consultation Paper assumes the cost could be between 1,318 and 3,145 billion pounds within 13 years,[61] while the German *Büro für Technikfolgenabschätzung* suggests that the initial expenditure could be up to 600 million euros, with annual costs up to 610 million euros, depending on the card technology and the distribution process.[62] In states such as Germany, where the validity period of the existing passport is ten years, the implementation of biometrics

---

[56] UK National Audit Office, "Introduction of ePassports", 17.

[57] UK National Audit Office, "Introduction of ePassports", 19.

[58] Bundesregierung, "Antwort auf die Anfrage der Fraktion DIE LINKE", *Bundestags-Drucksache* 16/161, 2005.

[59] See http://travel.state.gov/passport/eppt/eppt_2788.html.

[60] On the first version of the new passport in the UK (containing facial, but not yet fingerprint data), see UK National Audit Office, "Introduction of ePassports".

[61] UK Secretary of State for the Home Department, *Entitlement Cards and Identity Fraud. A Consultation Paper*, available at http://www.archive2.official-documents.co.uk/document/cm55/5557/5557.pdf, 2002, 131 ff.

[62] Büro für Technikfolgenabschätzung, *Biometrie und Ausweisdokumente*, 81 ff.

itself (*i.e.* regardless of the actual technology) could double the expenses: The ICAO recommends that the states consider changing the validity periods to five years for reasons such as technical flexibility and technology and security feature turnover. The German *Bundesregierung* announced that the validity period will not be shortened, yet it remains to be seen whether technical problems will demand changes in this respect.

There is great diversity among European countries concerning passport fees.[63] While Lithuania charges 60 LTL (approx. €17) and Spain €17, the UK's new passport costs between £66 and £114.50[64] (approx. €97 and €168), depending on the issuance process. Intermediate examples are Italy (€45)[65] and Germany (€59).[66] It is obvious from these examples that the total sum of fees paid by the respective citizens is not tantamount to the total cost of the passport system (which includes the production of passports, issuance procedures and enrolment equipment, readers at control stations, personnel and maintenance costs, and so on). Instead, an unknown amount of the costs will be paid for by the general budget.

In the end, the question of whether a project such as passports with biometric data will be accepted by citizens should not be underestimated. Given the potential to overcome legal and technical problems, this factor could be decisive for the realisation of such projects. However, acceptance seems to be a problem among human rights activists and data protection authorities, but, at least so far, not among greater parts of the population in the countries where biometric passports have been implemented.

5. Democratic Legitimacy: will the "European indirection" become the standard means to introduce new surveillance technologies?

It is apparent from the legislative procedure (see above 3.2) that the EU Council Regulation on Biometric Passports falls short of democratic legitimacy. The decision was made by the Justice and Interior Ministers of the EU member states, and it is very likely that not all of the national parliaments would have approved the new passports, particularly the storage of fingerprint data. As the European Parliament also opposed the use of fingerprints (leaving aside the problem of whether the Parliament itself is democratically legitimised),[67] this biometric feature is solely based on the decision of the Justice and Interior Ministers.

---

[63] See the survey of UK National Audit Office, "Introduction of ePassports", 31 f.

[64] See http://www.passport.gov.uk/fees.asp.

[65] http://www.poliziadistato.it/pds/cittadino/passaporto/pas2.htm.

[66] See Sec. 1(1) *Passgebührenverordnung* (available at http://bundesrecht.juris.de/passgebv_2002/BJNR 327500001.html).

[67] This is questioned on grounds of its marginal competences, the uneven representation of the respective people (see Art. 190 (2) TEC) and the doubtful existence of a European "demos", see R Fischer, *Das Demokratiedefizit bei der Rechtsetzung durch die Europäische Gemeinschaft* (2001), 72 ff. with further references (hereafter referred to as Fischer, *Demokratiedefizit*); P Häberle, *Europäische Verfassungslehre*, 2nd edn (2004), 311 ff. (hereafter referred to as Häberle, *Verfassungslehre*); W Kluth, *Die demokratische Legitimation der Europäischen Union* (1994), 44 ff.

These ministers are accountable to their respective parliaments for their actions in the Council. However, there is abundant evidence that in practice, the national parliaments are frequently neither involved in the decision-making process nor willing or capable of taking any action if the minister's voting behaviour does not represent the majority in the parliament.[68] Since courts such as the German *Bundesverfassungsgericht* have based the democratic legitimacy of EU law in large part on the accountability of the Council members to the national parliaments,[69] this is highly problematic. In the case of the EU Regulation on Biometric Passports, this is increased by the adoption of the ICAO technical standards, which are directly linked to the legal implications and practical problems of the new passports.[70] Through this process, the standards become directly binding for all EU member states.

Generally, the "European indirection" seems to be becoming more the norm for new surveillance measures. The latest example is provided by the EU Directive on Data Retention,[71] although in this case, the European Parliament was involved in the decision-making process. While the unification of law within the European Union is generally seen favourably, there is the obvious risk of shifting responsibility to the European level without providing for adequate processes of accountability: national government may claim to "only follow European requirements" when implementing measures of public security,[72] while they themselves made the crucial decision in the Council. The introduction of new surveillance measures might not be the only instance in which the EU's lack of democratic legitimacy becomes visible,[73] but it could become one of the most problematic examples of the near future.[74]

---

[68] Fischer, *Demokratiedefizit*, 114 f., 117 f. with further references.

[69] See Bundesverfassungsgericht, *BVerfGE* 89, 189 f.

[70] Roßnagel and Hornung, "Reisepässe", 989 f.

[71] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal 2006, L 105, 54 ff.

[72] See *e.g.* UK National Audit Office, "Introduction of ePassports", 8: "International requirements dictated chip design and the type of identifier on the chip".

[73] See generally Fischer, *Demokratiedefizit*; Häberle, *Verfassungslehre*, 306 ff.; P Kiiver, *National Parliaments in the European Union: A Critical View on EU Constitution-building* (2006); Bross, J.M., *Die Bedeutung des Grundsatzes der Demokratie für die Wirksamkeit europagemeinschaftlicher Sekundärrechtsnormen*, (1971), 134 ff., 186 ff.

[74] See also J Rauhofer, "Just because you're paranoid, doesn't mean they're not after you: legislative developments in relation to the mandatory retention of communications data in the UK and the European Union" (2006) *SCRIPT-ed, Journal of Law and Technology*, Vol. 3 Issue 4, 322 ff.