EUROPEAN PARLIAMENT

Directorate-General Internal Policies

Policy Department C

Citizens Rights and Constitutional Affairs

BIOMETRICS AND VISA APPLICATIONS

BRIEFING PAPER

Summary: The proposed Regulation amending the Common Consular Instructions as regards the taking of biometric data needs to be amended to ensure that biometric obligations are only extended to categories of visa applicants on a country-by-country and case-by-case basis following adequate justification in light of the objectives of the Visa Information System (VIS). There also need to be provisions in this Regulation (or the VIS Regulation) protecting the rights of applicants who are not able to enrol biometric data and addressing the issues of misused identity and technological failure. The use of biometric data in the VIS to identify persons should be subject to strict controls. Finally, there need to be strengthened provisions concerning the liability and monitoring of private companies which assist the Member States' authorities to process visa applications.

IP/C/LIBE/FWC/2005-08-SC3
PE. 378282 **EN**

This note was requested by: The European Parliament's committee on Civil Liberties, Justice and Home Affairs.

This paper is published in the following languages: EN, FR.

Authors: **Steve Peers, University of Essex**

Manuscript completed on 12 October 2006

Copies can be obtained through: Tel: 32105
Fax: 2832365
E-mail: joanna.apap@europarl.europa.eu

Informations on DG Ipol publications:
http://www.ipolnet.ep.parl.union.eu/ipolnet/cms

Brussels, European Parliament

VISA APPLICATION RULES

Steve Peers

INTRODUCTION

The following analysis examines key issues relating to the proposed Regulation of the European Parliament (EP) and the Council amending the Common Consular Instructions (CCI) on Schengen visas in relation to the introduction of biometrics for visa applications and the processing of visa applications. This is a parallel proposal to the earlier proposal to esatablish the Visa Information System (VIS; hereinafter the 'main VIS proposal')

BACKGROUND: VISA REQUIREMENTS

It should first of all be emphasized that persons who are exempt from a visa requirement will necessarily be exempt from the obligations set out in this proposed Regulation. The list of countries and territories whose nationals are (or are not) subjected to a visa requirement is set out in Regulation 539/2001 (OJ 2001 L 81), as amended.

Furthermore, this Regulation permits Member States to exempt from visa requirements refugees and stateless persons who hold a travel document issued by a country which is not subject to a visa requirement (Article 3) and children who reside in a country which is not subject to a visa requirement, when they are travelling on a school excursion (Article 4(3)) Conversely, a Member State may subject persons to a visa requirement, even if they would otherwise be exempt, if they carry out a paid activity during their stay (Article 4(2)). Member States may *either* impose a visa requirement *or* exempt from a visa requirement the following: the holders of 'diplomatic passports, official-duty passports and other official passports'; specified transport personnel; and 'the holders of *laissez-passer* issued by some international intergovernmental organizations to their officials' (Article 4(1)).

The Commission has published several communications on Member States' application of these exemptions (see most recently OJ 2003 C 68/2).

Also, the Commission has proposed a Regulation which would extend a visa requirement to one State and remove it from several others, and also amend the rules on exemptions (COM (2006) 84, under discussion in the Council and EP).

Finally, it should be noted that the EC-Russia agreement on visa facilitation exempts holders of diplomatic passports from any visa obligation (Article 10 of the agreement, COM (2006) 191). The agreement is not yet in force. The EC is also negotiating a visa facilitation agreement with Ukraine, and furthermore the Commission has asked the Council for mandates to negotiate such agreements with the Western Balkan states subject to visa requirements (Albania Serbia, Montenegro, Bosnia/Herzegovina and FYROM); the Council has also been considering the possibility of a visa facilitation treaty with Moldova. If such treaties are agreed and ratified, they may provide for further exemptions from the visa requirement.

BIOMETRIC REQUIREMENTS AND EXEMPTIONS

On top of the exemptions from the visa requirement (see above), the proposed Regulation would exempt from the fingerprint requirement (but not the photograph requirement) children under six years old and persons where fingerprinting is 'physically impossible'. Member States *may* exempt from *all* biometric requirements 'the holders of diplomatic passports, service/official passports and special passports' (Art. 1(2)).

The exemption from biometric obligations for children under 6 is consistent with the exemption of such applicants from visa fees in the recent Council Decision which amended the CCI to raise visa application fees (OJ 2006 L 175). However, the exemption from biometric obligations is narrower in scope than the other exemptions from the visa application fee under that Decision (as regards students, pupils, teachers and researchers, and, as an

option for Member States, on various public interest grounds or on humanitarian grounds). It is also inconsistent with the waiver of visa fees for nine categories of Russian nationals (see Art. 6(3) of the EC-Russia visa facilitation treaty).

The Commission admits that the exemptions are set out pursuant to an agreement in Council working groups and committees. It explains the exemption for children under 6 by reference to the lack of 'sufficient quality' of their fingerprints. Next, the Commission states that the fingerprints of 6-12 years are only suitable for a 'one-to-one' comparison. However, neither this proposal nor the VIS proposal restricts the use of such fingerprints to such comparisons. In fact, the EP's proposed amendments to the VIS proposal do not appear to address this issue either.

It should also be observed that since the age limits pursuant to the proposed VIS rules contradict the age limit of 14 agreed in respect of the Eurodac Regulation, the issue arises as to whether fingerprints of children under 14 pursuant to the proposed Regulation should be exchanged for the purposes of determining responsibility for asylum applications. This is relevant also where the fingerprints were taken before the child turned 14, but the child has turned 14 in the meantime.

Comparing the VIS proposal and this proposal, it appears that the most logical place to address the latter issue would be the main VIS proposal, in particular since the latter proposal regulates access to VIS data for asylum purposes in detail. Also, the most logical place to restrict the use of the fingerprints of children aged 6-12 would be the main VIS Regulation, since it contains rules on the access to and use of data, as distinct from rules on the initial collection of data (the essential purpose of the 2006 Regulation).

Another issue is comparing VIS biometric data to SIS biometric data, given in particular that biometric data for the purposes of the SIS will not be collected in the context of an immigration or document application process (ie, visas, passports or residence permits), and that the Commission's adoption of implementing measures concerning SIS biometric data is some way off (Art. 14a(3a) of the SIS II immigration Regulation). Moreover, the EP will lack co-decision powers over the adoption of this SIS measure; it has apparently not even pressed for the new comitology rules concerning quasi-legislative measures to apply to these decisions or any other SIS implementing decisions (see Art. 35 of the agreed SIS II Regulation). Furthermore, the SIS II Regulation does not contain age limitations regarding biometric data or limitations upon the use of biometric data concerning children aged 6-12 (unless the reference to technical feasibility in Art. 14C(c) of of the agreed Regulation is understood to incorporate this issue).

The Commission explains the optional exception from Member States by reference to the optional exception from the visa requirement for a similar (but not identical) category of persons (see above). However, this comparison makes little sense, for a person exempted from the visa requirement will obviously not have to apply for a visa and supply biometric data to that end in any case.

It would make more sense to assess the issue of exemptions from the biometric requirements in light of the purposes of the VIS. If it can be reasonably argued that a particular category of persons (for example, the elderly, a particular age group of children, or persons holding certain passports) do not represent a significant threat to any of the VIS objectives as set out in the main VIS Regulation, then it would not be necessary or proportionate to take their fingerprints and store them in the VIS. Indeed, the lack of necessity and proportionality of taking fingerprints for such persons would mean that taking their fingerprints would constitute an unjustified interference with their right to privacy pursuant to Article 8 of the European Convention on Human Rights and national constitutional principles.

Applying these criteria to just one case, there is clearly no link whatsoever between the objective of facilitating the application of the 'Dublin II' rules and the taking of fingerprints

of children under 14. The link between those childrens' fingerprints and the other objectives of the VIS would have to proved by the submission of sufficient evidence to that end.

The same sort of justifications would have to be provided for the subjection of any group of persons to the biometric requirements. Any exemptions justified on this basis should be harmonized, i.e. not an option for Member States, in light of the human rights arguments against interference with the right to privacy.

Furthermore, this proposal constitutes an opportunity for the EP to express a view on the question of whether the VIS (or at least the collection of biometric data) needs to be applied to all countries whose nationals are subject to a visa requirement, or at least to all countries on the time scale agreed by the Council (without any involvement of the EP or national parliaments, or any proper impact assessment) in its conclusions of December 2005. It could be argued that the extension of the VIS (or at least biometric data collection) to any countries, or groups of countries, or categories of persons, should be subject to an impact assessment based on objective evidence showing that the collection of biometric data is necessary in light of the pattern of visa applications from a particular country, and that any extensions of the VIS (or biometric data collection) must be subject to a fresh Commission proposal and approval of the Council and the EP (or alternatively a Commission decision taken pursuant to the new comitology rules for quasi-legislative measures).

It might be objected that such an approach would discriminate between countries or categories of persons. But (leaving aside the discrimination already inherent in subjecting some countries, but not others, to a visa requirement, in the absence of any objective standards to this end), EC rules already contain many distinctions between countries and categories of persons (as regards visa fees, visa facilitation policy, visa exemptions by different Member States, and the Schengen consultation procedure). A partial, differentiated application of the VIS (or biometric data capture) would also save resources for Member States which could be dedicated to measures that are more likely to protect security effectively, for example (such as improved intelligence and policing). Also, there would be fewer errors if the VIS database contains less biometric information.

USE OF BIOMETRIC IDENTIFIERS

From a data protection perspective, the biometrics issue has been addressed on a number of occasions by the EU's Data Protection Supervisor (EDPS) and by the 'Article 29 Working Party', which is made up of national data protection authorities and established by Directive 95/46 on data protection.

The EDPS elaborated upon biometric issues in his opinion on the VIS proposal (OJ 2006 C 181). In this opinion, he observes that if an identity theft is linked to a stolen biometric, it will be more difficult for the individual concerned to overcome the effects of this crime. Also, he observes that biometric data are not secret, and can be collected without the owner being aware of it. Finally, the EDPS, referring to studies, states that biometric systems are subject to a 5% rate of failure to enrol, and an error rate of up to 1%. The data provided in a footnote to the report appear to indicate that the rate of error in identification of persons by biometric means (a 'one-to many' search) will increase as the size of the database increases.

The EDPS suggests that a 'fallback system' be established where fingerprints cannot be taken. The proposed Regulation provides that in such cases, a 'not applicable' entry shall be inserted into the VIS; this matches Article 6(4a) of the main VIS Regulation as proposed by the EP. Inserting a 'not applicable' entry is obviously preferable than refusing a visa to all such applicants. However, there is a possible risk that applications will be refused at a higher rate from applicants who are unable to enrol biometric details. The best way to address this issue may be to insert an Article 10(2b) in the main VIS Regulation (immediately following the Article 10(2a) as proposed by the EP, which addresses comparable issues), specifying that the inability to enrol biometric data shall not in itself unfavourably influence a decision on the visa application.

It might be objected that provisions concerning the merits of a decision on visa applications should be inserted into the CCI, or the future Community code on visas, rather than into the text of the main VIS Regulation. But since the issue relates directly to the application of the VIS, it should be considered a matter ancillary to VIS legislation. Furthermore, the EC visa code may well not be agreed until 2008 at the earliest. It is necessary to regulate the issue in the meantime. If it is considered undesirable to address the issue in the main VIS Regulation, a provision concerning the effect of inability to enrol could be inserted as part of Article 1(2) of the 2006 proposal on the VIS and the CCI, or inserted as a new provision of the 2006 proposal amending the CCI, for example as a new point 2.5 of Part V of the CCI.

In his opinion on the SIS II proposals (Council doc 14091/05; OJ 2006 C 91), the EDPS inter alia comments on the level of accuracy of biometrics, noting in particular that the use of biometrics for identification 'are more critical because the use of this process is less accurate' than one-to-one verification. Biometrics should not therefore serve as a unique means of identification. More generally, the EDPS states that the SIS II proposal entails an 'overestimation of the reliability of biometrics' and that 'the accuracy of biometrics…will never be absolute', and refers to a case of false identification as a terrorist suspect that resulted in wrongful detention.

A widely available analysis of biometric technology, and in particular its potential use for border control, is set out in a 2002 report for the US General Accounting Office (GAO). The report states (at p 45): 'No match is ever perfect in either a verification or an identification system, because every time a biometric is captured, the template is likely be unique'. Therefore biometric systems are devised to search instead for an 'acceptable degree of similarity'. At page 55, after describing the concepts of false match rates (a 'false match' wrongly identifies a person as listed on a database) and false non-match rates (a 'false non-match' wrongly indicates that a person is *not* listed on a database), the report states that 'If biometric systems were perfect, both error rates would be zero. However, because biometric systems cannot identify individuals with 100 percent accuracy, a trade-off exists between the two'. At page 57, the report describes a third feature affecting the accuracy of biometric systems, the 'failure to enrol rate', which concerns people who for physical reasons are not able to supply a particular biometric. At page 71, the report states that fingerprints cannot be captured for between 2-5% of people; as for facial images, the report states at page 70 that a UK test showed a 0% rate of failure to enrol.

On the extent of accuracy, the report states at page 58 that 'because the performance of a technology depends greatly on how and where it is deployed, [the performance results claimed by biometric companies] have proven to be far more impressive than real-life performance data'. As to whether biometric systems can be fooled, the report states at page 62 that 'recent tests are casting doubt upon vendors' claims regarding the maturity and security of their technologies'; indeed '[f]acial, fingerprint and iris recognition systems were defeated by testers using photographs and videos, reactivated latent images and forgeries'. The report then refers to two further tests that defeated fingerprint recognition systems.

At page 69, the report summarizes the false match rates of facial images (0.3-5%) and fingerprints (0-8%), and also the false non-match rates of facial images (3.3-70%) and fingerprints (0.2-36%). Further statistics relating to various tests are given on the following pages.

In the Appendix to the report that examines fingerprint technology in detail, it is stated that although there is a 'widely accepted notion of fingerprint individuality', 'it has not been formally established by scientific means that a person's fingerprints are unique'. On pages 147-148, the report states that 'daily wear can cause the performance of some fingerprint recognition technologies to drop drastically'. It further refers to evidence that it is more difficult to capture fingerprint data from some groups (the elderly, manual workers and some Asian groups). Certain technologies have 'unique performance issues'. The false match rates

for the various fingerprint technologies used by US immigration authorities ranged between 1-4% (p 158).

Several of these points were reiterated in GAO testimony to congressional committees. In the published testimony, it is stated that '[n]o match is ever perfect in either a verification or an identification system' (at p. 6).

The GAO report is online at: http://www.statewatch.org/news/2005/apr/jrc-biometrics-paul-de-hert.pdf

The testimony is online at: http://www.gao.gov/new.items/d031137t.pdf

In light of these concerns (and the aforementioned concern about identity theft), it would also be desirable to insert into the main VIS Regulation a provision on misused identity, comparable to Article 25 of the SIS II Regulation. To deal with concerns about the error rate of the use of biometric technology, this provision must be broadened in the VIS context to apply also to cases of technological failure.

In order to prevent use of the biometric data for identification purposes before the technology is adequate, a provision comparable to Article 14C of the agreed SIS II text could also be inserted into the main VIS Regulation. This provision could even be strengthened in the VIS II Regulation; this could be justified in light of the additional data that the VIS database will contain, as this leads to an additional risk of errors in 'one-to-many' searches. A strengthened version of this provision would require a fresh decision by the Council, with the consent of the EP (or even a fresh legislative measure), taken in light of objective scientific evidence, before VIS data is used for identification purposes.

OUTSOURCING

The key issue as regards outsourcing is the liability of service providers towards applicants and the possibility of recourse by applicants against the service providers for providing inadequate service. The proposed Regulation does not require service providers to maintain any particular standards of service (except as regards fees) towards visa applicants. It is possible, for instance, that a legitimate visa applicant will be rejected because of an error made by the service provider, and in the absence of a requirement at present to motivate refusals of visa applications, it would be hard even for the applicant to determine whether the service provider was responsible for the refusal or not. Also, it is possible that a service provider could wrongfully refuse to process a visa application, behave unethically in extracting extra fees from visa applicants, or wrongfully encourage and then process a hopeless visa application (in the interest of collecting fees).

For these reasons, the Regulation must provide that Member States shall make service providers liable to visa applicants for errors, entailing the payment of appropriate compensation and shall require service providers to furnish to applicants all relevant information concerning the application in the event of any dispute or refusal of the application. Service providers must also be subject to judicial and non-judicial means of redress by applicants. The proposed provisions on information provided by service providers and consular posts should also be strengthened, in order to ensure that sufficiently detailed and accurate information, including information regarding redress in the event of disputes with service providers, must be provided.

From the perspective of Member State interests, it would also be useful to require Member States to keep a record of which applications were submitted by each service provider, and the rates of resulting visa refusals. This will provide objective information that could lead to a justified termination of the contract, or alternatively which the service provider could use to argue for its exoneration (or in order to explain the high rates of visa refusals). Of course, when compiling such records, any personal data that could identify applicants would have to be anonymized, as the processing of personal data would not be necessary for the purpose of assessing the reliability of the service provider. The collection of such information would

also deter service providers from encouraging hopeless visa applications purely in order to collect applicants' fees.

CONCLUSIONS

a) The Commission does not adequately justify the extent of the biometric obligations to be imposed upon all visa applicants. The EP should insist that the biometric obligations, and possibly even the application of the VIS more generally, must be approved by the Council and the EP on a case-by-case basis for certain categories of persons and certain countries on a case-by-case basis, pursuant to objective evidence linked to the objectives of the VIS;

b) In particular, there is no possible link between the fingerprints of children under 14 years old and the objective of facilitating the application of EC rules on responsibility for asylum applications;

c) It should be specified that the inability to enrol biometric data should not unfavourably affect a decision on a visa application;

d) The main VIS Regulation should contain provisions on misused identity and inaccurate identification due to technological failure;

e) A provision preventing the use of biometric data for identification pending technical confirmation and the approval of the EP should be inserted into the main VIS Regulation;

f) The proposal to amend the CCI should furthermore provide for the rights of visa applicants as against outsourced service providers, as well as strengthened provisions on information to be provided by service providers and consular authorities to applicants; and

g) A record of the applications submitted by each outsourced service provider should be kept, to provide objective information on the reliability of service providers.