An assessment of the proposed uniform format for residence permits

Sprokkereef, A.C.J.; de Hert, P.J.A.

Publication date:
2006

Directorate-General Internal Policies

Policy Department C

Citizens Rights and Constitutional Affairs

An Assessment of the proposed Uniform Format for Residence Permits

BRIEFING PAPER

Résumé: (Times new roman - text size 11 - maximum 15 lines)

Council regulation amending Regulation/(EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals provides for a uniform format for a residence permit issued as a stand alone document . This permit shall include a Radio Frequency Chip containing a facial image (within two years of the adoption of technical measures) and include fingerprints in interoperable formats (within three years).
The introduction of these two biometric identifiers in the residence permit is justified by the assumption that it is crucial in combating document fraud and fraudulent use to establish a more reliable link between the holder and the residence permit. This assumption is however not quantified in terms of the numbers of fraudulent cases which would be detected. Nor is there any acknowledged assessment of the ways the biometric identifiers chosen can be sabotaged or the system used fraudulently. In view of the many unknowns, such as the public reaction to being fingerprinted or the lack of experience in using these techniques at a larger scale, this is quite surprising. At the very least, in the amended proposal the disadvantages of using biometric identifiers at such a wide scale and at such an early stage in their technical development are not acknowledged to have been fundamentally assessed.
This note assesses the security measures chosen, analyses the impact of biometrics on the presumption of innocence, looks at the broader cost implications and is particularly critical of the decision to collect and store fingerprint data.

IP/C/LIBE/FWC/2005-xx

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: **Prof. Dr Paul de Hert (TILT, University of Tilburg) and Annemarie Sprokkereef (ICS, Leeds University and TILT, University of Tilburg)**

Manuscript completed 12th October 2006

Copies can be obtained through:

Tel: 32105
Fax: 2832365
E-mail: japap@europarl.europa.eu

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

Brussels, European Parliament

The authors would like to thank Prof Bart Jacobs from the Radboud University Nijmegen for his time in engaging in very helpful discussions in the process of writing this note. The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

A UNIFORM FORMAT FOR RESIDENCE PERMITS

INTRODUCTION

Since the adoption of the 2005 The Hague Programme the EU is set on a fast track of rapid introduction of biometric identifiers in passports and travel documents. The use of biometric technology in combination with increased availability and interoperability of data within the European Union are heavily relied on to enhance future security in Europe by making the identification of individuals and the verification of their identity more effective, reliable and cost efficient. On this road there is no turning back. We are past seriously considering the argument that by introducing biometric identifiers this early and without a proper public debate, we will forever alter the fundamental trust model between citizen and state, consumer and supplier. Serious concerns about the societal impact of the use of biometrics at a large scale (Ashbourn, 2005), the underestimated financial implications (LSE Report, The Identity Project, 2005), their technical feasibility (Council of the EU, note 15256/04) and LSE Report above), their susceptibility to large scale fraudulent use (The Register), their privacy implications (EP minority opinion, Carlos Coelho report A6-0029/2004) and the impact of the uncomfortable mix of the use of biometrics in civil and public sector applications (Jacobs, 2005) have not gathered the momentum needed to put a stop to the embracing of biometrics at governmental level. Governmental initiatives have been followed by frentic activity of economic and political stakeholders to find the technical solutions needed to make it seem to work, resulting in a plethora of sometimes completely un coordinated public sector schemes, in addition to the many civil applications emerging. This has gone hand in hand with the introduction of new increased powers of law enforcement activity. It is already clear that there is a lack of control over the emerging civil biometric databases, with a potential risk of uncontrolled matching or linkage to different databases in the future. It would make sense to take a distance, assess the broader situation and properly think through a well-coordinated and technically sound way forward. In fact, we are far from adopting a cautious approach to biometrics technology as a means to offer solutions to societal problems. Worse still, whilst a thorough public debate is absent we can find evidence of seemingly technically incorrect or even misleading rhetoric (Bio Metrics in Europe, trend report, June 2006; LSE report, 2005). Finally, what we risk by going about in this fashion also, is the gradual demise of the value of biometric identifiers for identification and verification purposes as a result of large numbers of biometric data, PKI codes, or even whole databases, falling in un authorised or even criminal hands.

It has to be stated here that the fact that there has not been broad, let alone public, debate on the subject is a result of political choice as made clear in the Presidency Note on the assessment of the state of the SIS II project in which it says that the Member States want to have a transparent discussion on the handling of biometric data in the framework of SIS II "without broadening it to a general discussion on the subject" 9672/05, 2nd June 2005). This observation should be taken seriously by the European Parliament in view of its specific tasks and powers. With the consequences of public resistance against the European Constitution in mind it would seem prudent to avoid making the same mistakes again by embarking upon a road without properly consulting, or at least informing, the general public.

Against this critical background we will now examine the Council regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals including its annex.

Technical solutions chosen

In short, the proposal provides for a uniform format for a residence permit issued as a stand alone document in ID1 or ID2 format. This permit shall include a storage medium (a Radio Frequency Chip, RFC) containing a facial image (within two years of the adoption of technical measures) and include fingerprints in interoperable formats (within three years of same). For a transitional period of two years after the adoption of the technical specifications

as mentioned, the residence permit may continue to be issued in sticker form. The proposal allows for the possibility to integrate a contact chip into the residence permit also, the use of which is optional. This chip should comply with ISO standards and shall in no way interfere with the storage medium. Finally, Art 4 now states that the biometric features in residence permits shall only be used for verifying the authenticity of the document; and the identity of the holder by means of directly available comparable features when the residence permit is required to be produced by law.

First of all, the new proposal maintains a reference to adhering to *the ICAO document No 9303 on machine readable documents* despite an objection from an EP rapporteur in an earlier EP report. He asserted that this document is constantly subject to change in a process which lacks legitimacy and transparency. This latter argument has to be examined against the fact that in many other policy areas standards are set by technical committees in the context of worldwide organisations not directly submitted to parliamentary control. Lack of transparency has for example never be held against telecom standards set by non government bodies.[1] Furthermore, the whole idea of worldwide compatibility already prevents constant ungradual changes being made to specifications set. The existence of the ICAO makes the work of the EU legislator more easy. Questions such as 'How will the biometrics be collected?' and 'What about their quality?' are simply answered with reference to the ICAO: *The taking of the biometric identifiers has to be carried out in accordance with the standards set out in the ICAO recommendations (Doc. 9303, part 1, 6th edition, not yet published). These standards set out in detail how the photograph has to be taken and give the standards for the scanning of fingerprints. No further technical specifications are required in order to ensure the harmonised enrolment of the biometric identifiers*.[2] In practice this means that the technical requirements are the same as for the passports delivered by Member States o their nationals in accordance with Regulation (EC) 2252/2004.[3]

The combination of a contact chip and a RFC (storage medium) on one card is technically compatible. A disadvantage of this solution is that the presence of the contact chip may limit the life cycle of the card. A contact chip normally lasts shorter because of the physical parts having to stick out to make contact with the reader. The issuing country can choose not to make the information on the contact chip readable for other member states. Technically, it would be possible however, to read and store the information on it when provided with the right key and encryption codes. A contact less card, incorporating a secure smart chip with a radio frequency contact less interface might have a 10 year life span according to the companies supplying them (The Register 30/1/2006) This will still have to be proven. Nevertheless, these assurances have taken away some of the concerns about the reliability of the cards. Nevertheless, the cost aspect in the longer term is still very unclear (*below*).

Although some of the following biometric identifiers: iris scan, hand geometry, vein patterns, signature verification, key stroke dynamics, voice verification, retina scanning and so forth, might be feasible for use in the medium to long term the identifiers chosen cannot reasonably be altered anymore, a discussion of other options will therefore fall outside the scope of this Note. The two identifiers chosen for the biometric passport and this proposal as well though, are in line with ICAO recommendations. In their review of biometric technologies, the ICAO assessed compatibility according to seven criteria, including: compatibility with enrolment

[1] What might be a much more pressing problem in this respect however, is that apart from the compulsory ICAO requirements there are also optional choices as to the technical specifications of documents. In the case of the biometric passport this has lead to some countries adopting these and some not. In the case of Germany this has resulted in the undesirable possibility to clone the biometric passport as demonstrated by security consultant Lukas Grunwald of German company DN-Systems (The Register). As the reliability of the system is determined by its weakest chain, this is a serious concern.

[2] Commission, Explanatory Memorandum, in *Proposal for a regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications*, Brussels, COM(2006) 269 final, 31 May 2006, (19p.) 3.

[3] Ibid, 15, footnote 5

requirements, compatibility with MRTD77 renewal requirements, compatibility with MRTD machine-assisted identity verification requirements, redundancy, global public perception, storage requirements and performance. The ICAO then assessed the available technologies based on their overall ability to meet the comprehensive set of requirements, and found that: face achieves the highest compatibility rating (greater than 85%) with finger(s) and eye(s) emerge with a second-level compatibility rating of near 65%. All other identifiers scored less than 50%.

Cost and security assessment

Facial biometrics

The facial image is held on a storage medium (RFC) on the permit. This is a high-resolution electronic portrait held on the chip as a photo, similar to the photos held on the new biometric passports. This allows for a visual check, comparing the person at the checkpoint with a display image on screen. The data can be accessed only after encryption, and the use of a Public Key Infrastructure (PKI) for authentication of data using an electronic signature, and like in the biometrics passports, only after some extra information is provided which can be found on the card itself. The latter is an additional check which prevents a cloned card being used which contains information that has been fraudulently obtained by illegal radiographic reading from a distance without access to the card itself. The equipment to do these checks should in fact already be installed at all border checkpoints in order to check biometric passports. What remains are the costs of installing this equipment at embassies and consulates.

As a certain quality standard should be respected (1000 ppi scanner) the costs for running the system will be high to extremely high. With the appropriate scans which can scan the info required for verification from the card, a routine check of a residence permit would not cost more than 30 seconds. In principle, the data inspected in this way can be stored on a computer and kept. They can therefore also be used for a facial recognition system check. This is a check of the image on the chip on the document against centrally held data, instead of against the person holding the card. For these kind of searches to be carried on hundreds of thousands of images in a centrally held database such as VISA, the computer hard and software needed is very costly and the process time consuming. Face recognition is in fact a long way from achieving the necessary accuracy for what is envisaged, and recent trials of the technology has shown relatively poor identification performance for even quite small populations, though it works well for one-to-one verification. While the combination of biometrics does allow for an improved performance, "the performance improvement is unlikely to be commensurate with the increased costs, and collection of the additional biometric images might be seen as unnecessarily intrusive by the public." (LSE Identity project, 2005)

Fingerprint biometrics

Fingerprints taken by live scan devices are most reliable when taken of 10 fingers. In the current proposal only two are provided for because of storage space available on the chip proposed. However, the error rate on two fingerprints is much higher than on ten. Article 1 of the proposed *Regulation amending the Common Consular Instructions on visas* obliges member states to collect ten fingerprints taken flat and digitally captured at the moment an applicant submits his/her first visa application.[4] Clearly this instruction allows for additional verification.

The problem with fingerprints is that they may wear with time and capturing requires touching a device. Rolled fingerprints (as practised in the USA), which are more reliable, require physical contact with the enrolling officer. In this context, it has to be remarked here that, in contrast to the recently introduces European biometric passports, and despite the excessive use of fingerprints for immigration purposes, USA passports do not carry

[4] Commission, *Proposal for a regulation of the European Parliament and of the Council amending the Common Consular Instructions*, *l.c.*, 14

fingerprints of USA citizens. Capturing fingerprints in civil applications using live scan devices with a resolution of 500 pixels per inch (ppi) does not offer sufficient resolution to be able to capture prints of sufficient quality for the EU residence permit. According to the manufacturers of the latest generation of scanners with a resolution of 1000 ppi these will be able to capture good fingerprints, also of those that have proved difficult in 500 ppi, such as children. These scanners have however not been tested in wide scale applications and independent experts question the optimistic prognoses of the market leaders in this respect. These 1000 ppi files require more storage capacity anyway; the size of the files will be 4 times the 500 ppi files (Trend Report 2006, p 19). The EU Commission has started the MIT project to study the interoperability of a standardized minutiae template (less than one kbyte), which could send images. The cost aspects of introducing these new scanners at all embassies and other points of enrolment have, to our knowledge, not been fully and publicly assessed.

Fingerprints can be forged and/or duplicated and applied to a finger in a very simple way, but also in more sophisticated fashions. Staff specially trained to detect this must therefore carefully monitor the capturing process. Even when being monitored it would be possible to make a false print with someone's fingerprint attached to the finger. Ideas of self-service capturing such as already in use in civil applications are therefore less desirable as possible abuse needs to be taken into account. Technical solutions to this problem might emerge in the not so near future, but have not so far. This touches a wider potential problem in that the ICAO stresses that machine checking of the document is not intended as a substitute for ID checking of the bearer. The ICAO systems are designed to impede the forgery or falsification of the document itself, and not to give any kind of guarantee that the bearer matches the document. For the time being we still need technology assisted border control and will have to rely heavily on human border guard capacity and skills, and training costs for border guards, embassy and other personnel will be high.

Fingerprints can be difficult to capture because fingers are too wet, too dry or too sweaty. Multi-spectral optical technology can overcome this problem but more severe are the difficulties with worn prints of fingers that have worn out because of daily use or on purpose to avoid a useable print. In addition, some people are physically less able to provide fingerprints (for example because arthritis) or mentally disturbed and/or unwilling to cooperate. It has to be acknowledged that a certain percentage of those requiring a residence permit cannot be fingerprinted for physical reasons.

Article 1 of the proposed *Regulation amending the Common Consular Instructions on visas* exempts from the requirement to give fingerprints:

– Children under the age of 6;

– Persons where fingerprinting is physically impossible.[5]

No alternative means as regards biometrics for these people are foreseen. Because we doubt the need for fingerprints as a second biometric in general (*below*) we welcome this.

Fingerprinting still very much carries a criminal stigma. Therefore, sabotaging of fingerprinting has to be counted in too, and as soon as this becomes an organised protest because of broad public resentment it can become a significant problem. Although there is new technology emerging (for example optical devices using spectral analysis: Trend Report June 2006, p 21) to help to overcome this problems they cannot be solved at a technical level yet. To avoid having to submit people to needless stress at the point of enrolment or border check point the use of an alternative bio identifier such as the iris scan could be considered. The cost aspect of this, as well as technical problems that go with it, will probably immediately rule it out. This then only leaves the option of exempting groups of people from fingerprinting. Which groups exactly will depend both on technical development and public

[5] Commission, *Proposal for a regulation of the European Parliament and of the Council amending the Common Consular Instructions*, *l.c.*, 16. If, however, fingerprinting of less than ten fingers is possible, the respective number of fingerprints shall be taken. A Member State may provide for exceptions from the requirement of collecting biometric identifiers for holders of diplomatic passports, service/official passports and special passports. In each of these cases an entry "not applicable" shall be introduced in the VIS.

acceptance. It is clear that in the case of visa and to a lesser extent, residence permits, individuals applying will be more vulnerable and less inclined to object than those applying for passports. However, if there is significant non-cooperation on biometric passports there might be a spill over on visa and residence permits.

Biometrics and the presumption of innocence?

One could question whether collecting data on the population at large (and not only on suspected persons) is reconcilable with the notion of the presumption of innocence and fairness. Intuitively, one would assume that the notion commands that only suspected persons are the object of state surveillance. However, the text of Article 6, paragraph 2 of the European Convention on Human Rights only envisages procedures of criminal law. It is only within such (formal) procedures that persons are presumed innocent, even when they are considered to be suspects. The presumption only protects persons who are labelled 'suspects' in order to bring them before a criminal court,98 it does not protect other persons (e.g. who are not suspect or 'suspects' who are not brought before a criminal court). Hence, the presumption is not operative outside the context of the traditional criminal procedure. Consider the example of biometric technologies used for security purposes. True as it is that the Court has condemned the use of broad terms in warrants and the lack of any special procedural safeguards in *Niemietz*,[6] the use of biometrics in large scale applications, such as border and airports checks, does not fit in a traditional scenario of criminal investigation.100 A broad, preventive application of biometrics will not, so we believe, be subjected to the *Niemietz* test. Note also that already with the 1990 Schengen Information System, requests for surveillance made by police and by national secret intelligence agencies, were made possible linking police interventions to a mere suspicion of danger. Seemingly Europe does not have too many problems with the lowering of the probable cause standard that is often imposed on traditional police work.

Secondly, since many of these contemporary strategies imply some sort of cooperation of the subject (showing a passport, giving data, enrolling in biometrical schemes ...), a discussion of *nemo tenetur* is not without logic. We saw that according to the Court the right not to incriminate oneself means that a suspect cannot be forced to supply evidence for his conviction and consequently the prosecuting authority has to collect evidence without the back up of items of evidence obtained by force or pressure. Can this be read as a prohibition of practices forcing someone to hand over biometrical traces or using biometrical traces against his will? *Funke* did not to seem to exclude this reasoning and there are precedents for this broad interpretation in the case law of some Member States.[7] However, the US Supreme Court rejected the broad interpretation and limited the *nemo tenetur* principle to the forced issuing of proof with a 'testimonial or communicative nature'.102 Apparently this case has served as guidance for the European Court which in the 1996 *Saunders* judgment opted for a limited interpretation: "The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, *inter allia*, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing".[8] This case law reduces the *nemo tenetur* principle to two very narrow concerns, viz. to protect the accused against torture

[6] In this case the European Court found a search and seizure in a lawyer's office to be a violation of the proportionality requirement that lurks behind the wordings of "necessary in a democratic society". After having found that the facts having triggered the investigation (pressure on a judge) were not of a minor nature, the Court noted the broad terms of the warrant and the lack of any special procedural safeguards, such as the presence of an independent observer in German law. Moreover the search impinged on professional secrecy to an extent that appears disproportionate in the circumstances. The Court then added the following: "it has, in this connection, to be recalled that, where a lawyer is involved, an encroachment on professional secrecy may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 (art. 6) of the Convention" (ECHR, *Niemietz*, § 37)

[7] ECHR, *Funke v. France*, judgment of 25 February, § 44.

[8] ECHR, *Saunders v. the United Kingdom*, judgment of 17 December 1996, § 68.

and to protect the judicial machinery from false statements made by the defence. In this narrow understanding, no other concerns are protected by the said principle.

Security of the biometrical data

Basically the biometrical data are protected by encryption codes,[9] which will be made available by the member state which has issued the card to those countries authorised to request it. Obviously the codes will be made available to other European Union states, but probably also to the USA and other states. As the codes will be used widely, the danger of abuse or disclosure has to be addressed in a serious way.

Here two dimensions should be distinguished: illegal use by authorised users and illegal use by un authorised users.

First, authorised users. Although it is technically possible to prevent inproper use of data to a very high level, there is always a price tag attached to this. Check and balances do cost staff time and therefore money. For example, the UK government has introduced a complicated multi layered authority level system in its recently introduced National Health Service life cycle data bank system. This system has turned out to be very expensive to run and is not feasible at the European level.

Second, unauthorised use. The storage of biometric data within the VISA system will be based on trust between third party nationals in (the authorised staff of) their guest member state, and subsequently on the trust of this member state in authorised staff in all other member states. In the first place, some systems are regarded more corrupt than others. Again here the strength of the system will depend on its weakest link. It is difficult to assess the risks of keys becoming public through mistakes in the various systems. Concerns have been heard, for example, about Polish plans to use mobile scanners at its borders with Russia. The argument is that these could fall in the hands of organised crime, including key codes and all member states would be affected.

Proportionality

Point 9 of the protocol on the application of the principles of subsidiarity and proportionality (TEU) states that "the Commission should duly take into account the need for any burden, whether financial or administrative, falling upon the Community, national governments, local authorities, economic operators and citizens, to be minimised and proportionate to the objective to be achieved".

The issue of the scale of the problem (administrative burden v problem/result ratio) as well as the financial burden on the third country citizen, border control agencies and enrolling points has received very little attention. The impact of the introduction of biometric identifiers is especially underestimated as regards the long-term effect of multiple storage of unique identifiers across a wide scale of civil and public applications. Identity theft through biometric identifiers cannot be avoided and a s a result of criminal use of these identifiers the reliability of both civil and governmental systems may decrease rapidly as a result. Regretfully, unlike passwords and despite the technique of templates, biometric identifiers cannot be reset.

Perhaps these burdens are still too far away to convince policymakers. Speaking at a public hearing in the European Parliament on 2 March 2004, António Vitorino, then European Justice and Home Affairs Commissioner, said appropriate use of biometrics would dramatically improve identification and protect citizens from ID theft. Mr Vitorino, who said he believed EU data protection laws are sufficient to safeguard citizen's rights, is convinced that high-tech identification systems will eventually protect European citizens and safeguard, not limit, their freedoms and rights. 'Biometrics will dramatically improve the accuracy of identification and protect citizens from wrong identification and having identification stolen

[9] The insertion of a contact chip where to store additional data (point 16 of the Annex) was proposed to make sure that the data are stored in a machine readable card instead of allowing the data to be read from distance. This contact chip will be purely for national use and cannot be read by other authorities. In Estonia the information on the chip will be the same as the information on an identity card carried by a national of the country. In this respect the contact chip (machine readable card) is regarded as safe. It is however, slightly more subject to wear and tear.

by someone else,' he said, adding that the Commission's goal is to find reliable and efficient measures to 'support the free movement of persons'.[10] The Commissioner highlighted the successful work of the Eurodac fingerprint database for the comparison of fingerprints of asylum applicants and illegal immigrants, saying that out of 250,000 identifications there has not been one 'false positive' ID.[11] At the same occasion, European Parliament's rapporteur Ole Sorensen voiced concerns about the implementation costs of biometric systems, 'which are likely to be very expensive for Member States'.
Higher we pointed at lack of information about short-term costs, e.g. costs of installing high quality standard equipment at embassies and consulates. Although the proposed *Regulation amending the Common Consular Instructions on visas* addresses some important organisational aspects and creates new possibilities for the organisation of the visa application procedure in order to enable Member States to cope with the additional workload of collecting the biometric data of applicants and to reduce the costs, these costs will inevitably increase at least for the applicant,[12] and the member states that will have to buy the technology needed for the biometrical systems. Techno-optimism is not a good option and happens to mislead policy makers.[13] Above we refuted the argument advances by some experts on border controls that the system will have the effect of the employment of less humans to make up for increased costs. The ICAO rightfully stresses that machine checking of the document is not intended to substitute for ID checking of the bearer. A similar guideline can be derived from the case law of the Court of Justice. In a recent case relating to the use of the SIS (the Schengen Information System), the Court of Justice declared that Spain infringed the right of free movement of family members of EU citizens, by refusing entry to a person into the Schengen area and by refusing to issue a visa for the purpose of entry into that territory to this person and his wife, nationals of a third country who are the spouses of Member State nationals, *on the sole ground that they were persons for whom alerts were entered in the Schengen Information System for the purposes of refusing them entry, without first verifying whether the presence of those persons constituted a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society*.[14] The applicable Council Directive 64/221 (Article 3) - which Spain infringed - stated that "measures taken on grounds of public policy or of public security shall be based exclusively on the personal conduct of the individual concerned" and that "Previous criminal convictions shall not in themselves constitute grounds for the taking of such measures."

The foregoing brings us to the question whether all the ingredients of the current proposal, including a) not one but two biometric features (with fingerprints not being chosen in the USA and traditionally reserved for criminals), b) systematic and centralised storage of sensitive personal data and c) secondary use, does not amount to a disproportional heavy reaction against a problem that lacks empirical analysis: Does the threat to public order justify measures of this kind? Equally, objectives are centred on the idea that catching criminals or illegal immigrants at border controls will turn them away, and discourage others.

---

[10] António Vitorino, also voiced the opinion that biometrics, 'like any other technology', is not dangerous in itself". 'It is the use you make of technology that might endanger fundamental rights', he added. Considering that Europe must 'face up to technological developments' and 'regulate these developments by making best use of them instead of avoiding or ignoring them', the Commissioner also held that EU data protection laws were sufficient to safeguard citizen's rights. The 1995 EU data protection directive indeed applies to the processing of personal data- including biometric data- by member states' authorities within the scope of Community law. This note will not comment any further on the more technical data protection aspects of the present proposal.

[11] 'European Commissioner highlights benefits of biometric passports', *eGovernment News*, 4 March 2004, 2p. via http://europa.eu.int/ida/en/document/2221/355

[12] Visa was 35 Euro now 60 Euro (Decision 2006/440/EC of 1 June 2006 amending Annex 12 to the Common Consular Instructions and Annex 14a to the Common Manual on the fees to be charged corresponding to the administrative costs of processing visa applications *OJ L* 175)

[13] The LSE Identity project identified the costs related to including biometric identifiers that the UK government had failed to consider carefully or underestimated severely. Most of these also apply to this proposal and include the true and realistic costs of: biometric equipment, validity period of the permit, enrolment, card replacement, non-cooperation, updates, integration costs, other public sector costs (training, communication) and the choice of reliable technology (The Identity project, LSE, 2005, p 158).

[14] European Court of Justice, Case C-503/03 (Commission v Spain), Judgement of 31 January 2006, available through http://curia.eu.int/.

What is the percentage of extra hits needed to achieve this? How does this compare to the costs, time of ordinary citizens and intrusion of privacy involved? More importantly, is this how it will work out? Maybe this will just divert the flow of bad guys but not stop it.
The current proposal is partly a copy past exercise of some of the choices behind the European passport. Elsewhere we have demonstrated that these choices, in particular the requirement of fingerprinting (not demanded by the U.S.), can only be understood in the light of a secret law enforcement agenda to establish a centralised database or a network of databases with fingerprints of the larger majority of the European citizenship.[15] As long as this hidden agenda is not put to the test of public debate, there is no doubt about the disproportional character of some of the elements in the current proposal.

Conclusion

The 2005 LSE report (The Identity Project) on the introduction of ID cards in the UK concluded: The consequences of the current proposals might include "failure of systems, unforeseen financial costs, increased security threats and unacceptable imposition on citizens." It is not that difficult to argue that this statement can also be applied to this proposal. As regards the introduction of bio identifiers in residence permits, this proposal does not seem to impose any extra burdens on third country nationals compared to EU citizens, but for one important aspect, viz. the inclusion of their data on the VIS database
This note has been in particular critical of the decision to collect and store fingerprint data. Finger prints can be forged and/or duplicated and applied to a finger very simply, but also in more sophisticated ways. The capturing process must therefore be carefully monitored by staff specially trained to detect this. Even when being monitored it would be possible to make a false print with someone's fingerprint attached to the finger. Technical solutions to this problem might emerge in the not so near future, but have not so far. Machine checking of the document is not intended to substitute for ID checking of the bearer.
In the context of the European passport an identical choice for fingerprints was made. Assuming that public acceptance regarding fingerprinting is low, some protest can be expected whenever the first passports are delivered. It is clear that in the case of visa and to a lesser extent, residence permits, individuals applying will be more vulnerable than those applying for passports. However, if there is significant non cooperation on biometric passports there might be a spill over on visa and residence permits.

Some have very convincingly argued we should first have a proper public scrutiny and debate on the social implications of wide scale implementation of biometric and related technologies by those most qualified to offer an opinion. Only then would we be in a position to develop a positive and trustful approach to biometrics and to decide on whether to introduce biometric or other measures. (Julian Ashbourn, 2005) This approach would be based on an analysis of the economic and social costs of the introduction of biometrics now against the potential benefits it could bring. The question whether it is efficient to invest in checking all travellers extensively at large economic and social costs in order to stop the influx of illegal immigrants needs answering. Another fundamental question is whether the technology is ready for wide spread use and whether government use of biometrics sits comfortably with civil applications. Is there an end to the places that can store our fingerprints? How much are our other fingerprints worth if one of them gets in the wrong hands? Will we shoot in our own foot? Can we still jump off the biometrics bandwagon anyway?
Another, drastic change of policy would be to abandon all contact less technology measures but to rely fully on *on card* verification. This places 'law abiding' citizens (which form the large majority of EU border crossers) in control of their own data without compromising on privacy or risking the loss of the legal or economic value of their biometric identity. Large scale theft or loss of data with potentially enormous consequences could than be excluded.

[15] DE HERT, P., 'Legal Aspects of Biometric Technologies', in residence' in INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES - JOINT RESEARCH CENTRE, *Biometrics at the Frontiers: Assessing the Impact on Society*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Homme Affairs (LIBE), February 2005, IPTS-Technical Report Series, EUR 21585 EN, p. 75-85

Although individual pda type devices would be costly, the infra structure needed to use them would be more economical.
Effective safeguards to prevent the handling of the contact less data accessed at border points for purposes other than the original check of identity and verification should be spelled out and agreed on. Especially, clear European rules for any searches or passing on of data stored should be put in place. As practices differ considerably from country to country this can not be achieved in the short term.