

European Biometrics Forum

2 October 2007

The implications of using biometrics in the VIS

Baroness Sarah Ludford MEP

Thank you for inviting me to take part in this interesting seminar on an issue raising so many important policy and technical questions.

The VIS is the third major information technology-based system to be established within the area of freedom, security and justice. The development of large scale biometric databases at the EU level in the field of border control, immigration, asylum and security and their possible synergy is a top EU priority. The Schengen Information System and Eurodac databases are already in place, and the VIS and SIS II are expected soon to become operational too. Other biometric databases such as an entry-exit system, a trusted traveller system, a criminal automated fingerprints identification system (EU-AFIS), a passport and ID cards register are also under discussion.

We are also confronted with increased demands of access by law enforcement authorities to immigration and asylum databases, such as access to the VIS or to Eurodac databases. We need a wide discussion on the implications of all these new technologies on privacy and civil liberties. The UK House of Commons has started an inquiry into the growth of a surveillance society and I would very much like to see something similar at the EU level.

Let me now say a few words about my own experience in this area, being the European Parliament's rapporteur on a far reaching project, the Visa Information System, and on a related proposal on collection of biometrics.

Background: VIS the biggest biometric database in the world

The main purpose of the VIS is to improve the common (Schengen) visa policy by facilitating the exchange of information between member states on short-stay visas. It will be based on a centralised architecture, with a central database where all information is stored and national interfaces located in the Member States allowing their competent authorities to access the central system. The system will lead to a huge collection and processing of personal and biometric data. Information on approximately 20 million visa applicants

will be stored annually in the system and with a five year retention period, this could lead to no less than 70 million fingerprints data stored at any one time. The VIS will be the largest biometric database in the world when it starts, although US-Visit will no doubt overtake it because of its very long retention period. Access to the system will be given to visa, immigration, asylum and border control authorities but also to member states' police and intelligence services as well as Europol for the specific purpose of fighting terrorism and serious crimes.

As rapporteur on the VIS my goals have been to make sure that the system should have clear purposes, rules and responsibilities in order to minimize the risk of abuse or malfunction creating harm to people. My main concerns were function creep and the use of data not for specific checks but for data mining, fishing expeditions, profiling etc. After nearly a year and a half of often tough negotiations, I believe we achieved a sound and balanced result with a system we can have confidence in.

Biometrics in the VIS

I am now dealing with the related and sensitive proposal of collection of the biometrics needed in order to make the VIS operational. There are two elements in this new proposal of particular concern and which are currently under intensive discussion with the Council and the Commission. These are the age limits for the collection and use of biometric identifiers (fingerprints and photographs to be used for verification and/or identification purposes) and the outsourcing of part of visa handling process to external service providers. Both elements have a considerable impact on data protection and I will come back to them later.

Specific nature of biometric data

The impact of the use of biometrics in such a large system is going to be significant, in particular on the privacy of a great number of individuals but organisational and technical challenges. There are many questions, both political and technical ones, which need an answer.

For example, how reliable are biometrics in such a huge system as the VIS? What are the appropriate age limits for accurate and usable fingerprints and photographs, those meeting the test of being necessary and proportionate to the purposes of the system? What safeguards do we need for the cases of inability to register biometrics or remedies for failures of the system?

European Data Protection Supervisor Peter Hustinx, in an opinion from March last year rightly said:

“Biometrics are not just another information technology. They change irrevocably the relation between body and identity, in that they make the characteristics of the human body “machine-readable” and subject to further use. Even if the biometric characteristics are not readable by the human eye, they can be read and used by appropriate tools, forever, wherever the person goes”.

Biometrics are not and cannot be the absolute solution in the search for more security, they are not the magic bullet. There are technical imperfections and the risk of error could be high. To put over-reliance on them could deliver exactly the opposite of the reassurance sought.

The widespread use of biometrics will have a major impact on society and should therefore be subject of a careful reflection and a wide debate before laws and systems are set up. Given the extremely sensitive nature of biometric data, stringent safeguards must also be put in place. The introduction of biometrics in the VIS will substantially change the shape of the visa policy and it has also the potential to affect people's lives quite strongly..

There are both advantages and disadvantages with the introduction of biometrics in the VIS:

On the one hand, biometrics are expected to facilitate a more thorough examination of visa applications, facilitate reliable identification and verification of travellers, thus reducing visa fraud and illegal immigration and making a contribution to internal security in general.

But on the other hand, the inclusion of biometrics in the system will lead to significant financial costs and to potential increases in the visa fees for applicants, and will have a very significant impact in terms of convenience for applicants, privacy and human rights.

A word on two important and sensitive issues regarding the introduction of biometrics into the VIS that I already referred to, the age limits for fingerprinting and the question of outsourcing of parts of the visa procedure to external service providers.

Fingerprinting children and the elderly

There is not only a question of technical feasibility in using fingerprints of children and elderly people, but also a question of what real benefits this would represent for the implementation of the VIS and an issue of proportionality.

Unfortunately the Commission has not carried out any such assessment; there was no impact assessment specifically for the collection of VIS biometrics. The age limits it has proposed: from 6 to 12 only use for verification, though that was not explicitly stated in the legal binding text, and from 12 onwards with no upper limit use for both verification and identification, largely reflect discussions which took place only with the Member States in the Council.

With no serious assessment of the technical feasibility or value of taking fingerprints from such young children, I cannot accept the simplistic argument that we have to do it in order to fight against child trafficking. I am proposing to the Commission and Council a serious examination, to see if clear evidence demonstrates necessity, proportionality and feasibility. It may be that the conclusion of that exercise points to taking fingerprints from children even younger than 6 years old, as children are trafficked well below that age.

As regards the elderly, the Commission does not propose any upper limit. I do not accept the argument that it is discriminatory to exclude them, in my opinion it is a justifiable distinction. Firstly, elderly people in general are very unlikely to be an immigration and terrorism risk. I am told Member States fear their welfare systems suffering an invasion of elderly from third countries passed off as grannies and grandads. But without some qualitative assessment of the real dimensions of such a problem, I really do not see it as proportionate to burden every old person of 80 and more with the obligation to travel and queue to provide their fingerprints. There is a question of the image the EU wants to give to the outside world in terms of respect for old people.

There is a policy decision to be taken on age limits, one based both on technical reliability and on privacy-intrusion considerations. But that needs credible assessments and experiments, currently lacking. Some say we cannot use the age limits of Eurodac and US Visit system as the basis for the choice of the age limits in the VIS since the age limit of 14 in Eurodac was based on then-existing commercial advice and US-Visit has a more limited purpose than the VIS. But we need more than opinions on which to base a rational choice of different age limits in the VIS. Eurodac and US-Visit are the only working systems in operation and we cannot run the risk of turning the

VIS itself into an experiment. I would recall that such a mistake was done in the case of the chip to be included in Schengen visas and residence permits, when it was discovered only at a very late stage that the solution envisaged was technically impossible.

The brochure of this very conference says "while some countries host key players of the biometric industry and have conducted various biometric tests, other countries are procuring large-scale passport and visa projects without significant experience in the field." I put to you that this is a worrying situation, and one that could rebound eventually with a public loss of trust if things go wrong in terms of misuse of data or breach of data security. This could also lead to loss of commercial opportunities, so it is very much in the interests of the industry that we build biometric systems on technically sound, well-proven and privacy-respecting technologies.

It is my strong belief therefore that the EU institutions need and should commission an in-depth study on age limits which could be a very useful instrument also in other contexts, given the current lack of credible and independent information regarding the challenges of fingerprints. For example, Professor John Daugman at Cambridge University quoted, during a recent BBC programme on ID cards, worrying statistics about fingerprint error rates. I have sent a letter, together with my colleagues from the other political groups, to Vice President Frattini and the Portuguese Presidency proposing an independent and objective study, and we await a reply.

Outsourcing

The inclusion of biometrics in the visa issuing process also means that all visa applicants, at least for the first application, will be required to appear in person at consular posts to provide their biometric data, and this brings me to the question of outsourcing.

Outsourcing to external service providers could indeed be a solution in order to facilitate applications and release applicants from an extreme burden of travelling long-journeys for getting to a consular post. However, given the sensitivity of the biometric data involved, and the potential risks for both physical security of the data and data protection, it is legitimate to ask whether the processing of visa applications by an external service provider in a third country is indeed appropriate.

It is clear that a poorly-managed outsourcing with no adequate data protection and data security safeguards could present considerable risks for individuals and for the integrity of the whole visa-issuing process. The recent

UK independent report on the breach of data security in the online application facility operated by VFS in India, Nigeria and Russia on behalf of UKvisas confirmed that these risks are far from being abstract ones.

The Swift affair of banks being forced to hand over financial information to the US authorities also shows how dangerous is to be subjected to the national law of the third country where a service provider is established. And many will be in countries with regimes that are distinctly unsavoury.

We as legislators have the duty to make sure that safeguards are in place to ensure full respect of data security and data protection and in my draft report I have tabled a series of amendments to try and ensure this, as they are essential components of fair and efficient visa system. The challenge is of course in finding a solution which is also convenient for visa applicants.

I also want to ensure that outsourcing will not increase visa costs for applicants. Some Member States, practising outsourcing without any legal basis for doing so, have already increased fees. This is unacceptable and I strongly encourage the Commission to bring infringement procedures against them.

I have no prejudice against private suppliers, but given the possible risks of outsourcing I believe it can only be admissible as a last resort and when there are full guarantees for data security and data protection, such as location in a place protected under diplomatic status, and where there are strong contractual clauses providing for oversight and liability of the contractor.

Let me conclude by saying that it is vital to get the VIS system right, but it is equally important to see it in the wider context, characterized by the increase use of biometrics at EU level and in particular the development of other large-scale IT databases and their intended interoperability. All this is a highly sensitive area, with considerable risks for infringing privacy and other fundamental rights. If all these measures are not carefully considered with due regard to necessity, privacy and proportionality, they risk instead of creating a safer society to be midwife to a surveillance society. That is one in which no-one could feel safe because no-one could feel free. As we say in colloquial English, that is not my cup of tea!

Thank you again for inviting me to speak and I am happy to respond to comments or try to answer any questions you might have.