NOTE

DIRECTORATE GENERAL INTERNAL POLICIES OF THE UNION

EUROPEAN PARLIAMENT

Policy Department C
Citizens Rights and Constitutional Affairs

A comparison of the now agreed VIS package and the US-VISIT system

BRIEFING PAPER

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

JULY 2007
PE 378.306

EN

PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU EURÓPSKY PARLAMENT
EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Directorate-General Internal Policies

Policy Department C

Citizens Rights and Constitutional Affairs

A comparison of the now agreed VIS package and the US-VISIT system

BRIEFING PAPER

In recent years, U.S. and EU have both set up border-related database systems with striking similarities as regards names and major development phases occurring in the historical context of post-9/11. Nevertheless doubts are appropriate as to how far the parallels go between the European VIS finally adopted as an instrument of the common visa policy and US-VISIT known for its dedicated role in the "war against terrorism".

On the basis of a detailed examination of systems and contextual features, the present briefing undertakes to illustrate major divergences in terms of underlying purposes and means employed which once again confirm well-known transatlantic divides as to the significance of data protection, availability of data to a wide range of security authorities, perfectionist use of biometric control processes etc. The transatlantic comparison also takes note of rather disillusioning experiences made by US-VISIT: despite deployment of enormous financial resources, newest technology and the envisaged use of accompanying measures such as ETA, the modernisation of the Visa Waiver Program (VWP), the seamless protection of US borders appears still not in sight. Certainly a lesson to be retained in view of possible European ambitions to follow the U.S. on the same path!

IP/C/LIBE/FWC/2006-202/LOT4/C1/SC1

This study 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: **Dr Peter Hobbing, CEPS**

Manuscript completed in (4 July 2007)

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

TABLE OF CONTENTS

A comparison of the now agreed VIS package[1] and the US-VISIT system

Peter Hobbing[2]

Introduction

Not only the similarity of acronyms make European VIS and American US-VISIT[3] seem to be "cut from the same cloth" and appear "almost like twins". The impression of a close relationship is reinforced by the treacherous assumption that both systems were born in direct response to the events of 9/11 – whereas in reality their roots lie elsewhere.

Others, however, consider them as "different as lemons and apples" pointing to quite diverse objectives pursued ("facilitation of the common visa policy" on VIS-side as opposed to the "fight against terrorism" prioritised by US-VISIT).

In any case, both systems have undergone remarkable evolutions, with some sharp turns and complex clusters of regulatory objectives included, which would defy any one-dimensional classification. Beyond all underlying philosophy and factual orientation, the comparison between both mechanisms also pays off in view of the striking parallels on the practical side, notably biometry-based identity controls and their impact on privacy and data protection. We thus may learn some transatlantic lessons from each others experiences, successes as well as actual/foreseeable failures.

At the same time, the study provides some additional insight into most recent developments in transatlantic air travel including the PNR arrangements as a longstanding "bone of contention" between EU and US as well as the newly proposed Electronic Travel Authorization and the intended modernisation of the Visa Waiver Program (VWP).

1. VIS and US-Visit compared

The comparison undertakes to cover all relevant aspects of the systems concerned, whereby this should usefully extend beyond the individual aspects of positive legislation to equally include a few thoughts on the history and other significant factors explaining the diverging approaches on travel and border control.

1.1 Border controls in the light of changing purposes and expectations

Migratory pressure, fear of crime and other paramount societal concerns – though often in rapidly changing configurations – traditionally shape the character and intensity of border controls. Clearly the attacks of 9/11 have had a very significant impact on the development of both systems, especially of course in the US, but they did not trigger off their actual creation.

US-VISIT exists since 1996 when it was designed as a tool of "immigration law" [4], notably by identifying visa overstayers but it was recast in 2001 notably by the US PATRIOT Act[5] in order to play a prominent role in the fight against terrorism. Also the planning of **VIS** started before 9/11, while it became a political priority only on 20 September 2001 when EU justice and home affairs ministers decided to launch a "network for information exchanges concerning the visas issued"[6]. The post-9/11 period was then marked by

[1] It is noted that the VIS package consisting of VIS-Reg and VIS-D07 has not yet been formally adopted at Council level, although full agreement on the content was reached on 14 June 2007. Legislative references refer to the texts published at the EP website: http://www.europarl.europa.eu/sides/getDoc.do?Type=TA&Reference=P6-TA-2007-0227&language=EN; http://www.europarl.europa.eu/sides/getDoc.do?Type=TA&Reference=P6-TA-2007-0229&language=EN

[2] Dr Peter Hobbing is a Senior Associate Research Fellow at the Centre for European Policy Studies (CEPS). The usual disclaimer applies.

[3] US-VISIT=„U.S. Visitor and Immigrant Status Indicator Technology", cf. Koslowski (2005), p.1; VIS= „Visa Information System", cf. Art. 1 VIS-D04

[4] IIRIR Act (1996) („Illegal Immigration Reform and Immigrant Responsibility Act"), sec. 110; cf. Koslowski (2005), ibid.

[5] USA PATRIOT Act (2001): SEC. 414.

[6] EU Council (2001), Conclusion N° 26

lengthy skirmishes as to what extent VIS would also serve to the purpose of law enforcement and antiterrorism[7], before the VIS package now adopted the priority of visa over law enforcement objectives.

1.2 The current purposes

Although neither of the systems is one-dimensional in the sense that it would exclusively pursue either immigration/visa or law enforcement purposes, the characterization of **US-VISIT** (primarily protection against mobile terrorism) and **VIS** (primarily support of the common visa system) seems obvious given that the underlying legal provisions are clear-cut in establishing hierarchies between the various objectives.

While US-VISIT prioritises "the security of our citizens and visitors" over the facilitation of travel and trade, integrity of the immigration system and the privacy of visitors[8], VIS puts the "implementation of the common visa policy" in first place (Art. 2 top and paras (a) to (f) VIS-Reg.)[9], well ahead of the "prevention of threats to internal security" (Art. 2 (g). VIS-Reg.)[10]

1.3 Structure of the law

For various reasons, last but not least different traditions, the legal instruments in question defy easy comprehension. Both appear in rather scattered formations of three or more separate laws. While the EU split (VIS Regulation vs VIS Decision) according to subject matters and competence corresponds to our well-known 1st – 3rd Pillar gap, we have some more difficulties in understanding the American structures.

Since 1996, the US-VISIT system has been amended four times by the Immigration and Naturalization Service Data Management Improvement Act of 2000[11], the US Patriot Act of 2001[12], the Enhanced Border Security and Visa Entry Reform Act of 2002[13] and the Intelligence Reform and Terrorism Prevention Act of 2004[14] (with further amendments pending)[15]. There are, however, no consolidated texts and other familiar tools facilitating the comprehension of complex legislation (eg. „statement of reasons"/„exposé de motifs", references to provisions changed/replaced/abolished in the original text). Even official government guidelines and academic articles provide no clue as their very helpful and elaborate statements are normally not accompanied by explicit legal references. This factor is being emphasized mainly to explain why the comparison" in legal terms" as requested by the EP assignments encounters some unforeseen difficulties.

1.4 Scope of application

It is well in line with the characteristic features established above (protection against terrorism vs support of the common visa system) that **US-VISIT** since end 2004 has abolished the privileges of the economically advanced VWP countries[16] which do not present a specific threat in terms of illegal immigration to the US. Currently only Canadians and certain groups of Mexican citizens are exempt from the enrolment requirement (cf. DHS, 2006).

[7] cf Hayes (2004)
[8] DHS US-VISIT (2005), p.2
[9] This includes the following individual visa-related purposes: (a) to facilitate the visa application procedure; (b) to prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application; (c) to facilitate the fight against fraud; (d) to facilitate checks at external border crossing points and within the territory of the Member States; (e) to assist in the identification of any person who may not, or may no longer fulfil the conditions for entry to, stay or residence on the territory of the Member States. Another purpose concerns the **asylum** system, i.e. (f) to facilitate the application of Regulation (EC) No 343/2003.
[10] Art. 2 VIS-Regulation
[11] DMIA Act (2000)
[12] see Fn. 4 above
[13] EBSVER Act (2002), Sec. 302
[14] IRTP Act (2004), Sec. 7208
[15] see overview at GAO (2006), Appendix III
[16] US-DoS (2006); Immigration and Nationality Act (U.S.C. 1187), Sec. 217 (c)(2)(A)

The **VIS** approach is more modest insofar as it addresses only those third country nationals subject to the Schengen short term visa requirement; this means that in fact citizens of currently 29 industrialised countries[17] are exempted from the system.

1.5 Types of data stored

Both systems require biographical as well as biometric data.

US-VISIT in terms of biographical data requires name, date of birth, document numbers, etc contained in a machine-readable passport as defined by ICAO[18] as well as elements relating to the current trip[19]. The biographic data required consists of **two** index fingers digitally scanned and a digital photo taken at the U.S. port of entry (DHS, 2007). The biometric standards used correspond to those established by the National Institute of Standards and Technology (NIST)[20]Regarding US plans to upgrade the fingerprint requirement to ten fingers, see Section 2 below.

The respective requirements for **VIS** are explicitly listed in Articles 9 - 14 VIS-Reg, i.e. in terms of biographical data this includes elements relating to the visa issuing procedure (Art. 9 (1)-(3)), to the person of the applicant (Art. 9 (4)) and to certain situations arising afterwards: issuance of visa (Art. 10), visa examination discontinued (Art. 11), refusal of visa (Art. 12), revocation/ annulations of visa, shortening of validity period (Art. 13, extension of visa (Art. 14). Regarding biometric data, the requirements are a digital photograph, in compliance with Regulation (EC) 1683/95 and thus ICAO standards (Art. 9(5)), and digital fingerprints (Art. 9(6) in conjunction with the Common Consular Instructions, CCI), whereby the **ten**-finger-requirement is part of still a pending proposal for amending the CCI[21].

1.6 Availability of biometric data

The accessibility of biometric data by internal security agencies having been one of the hot spots of the European legislative debates (cf. Ludford, 2007), it is remarkable to see that this aspect has troubled Americans much less. The "transatlantic divide" may well be explained by the different placement value granted to the "war" (or not) against terrorism (van Herpen, 2004).

As an initiative with a strong if not predominant law enforcement component, **US-VISIT** data from IDENT or other databases, including their biometric components, are routinely available for sharing with other DHS components as well as "other law enforcement agencies at the federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting law enforcement intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders" (DHS 2003, p. 5). The requirement that the disclosure is compatible with the „purpose for which the information was collected" (ibid.) appears a mere formality given that all before-mentioned authorities belong to the law enforcement/security branch. However, restrictions, including "data access controls, need-to-know and existence of Memoranda of Understanding" (DHS US-VISIT 2007) evidently play a vital role with regard to a yet wider list of possible recipients established by DHS US-VISIT[22] (ibid).

If there is any resistance, it would rather come from the local level, where cities such as New York with an important share of immigrant population do not subscribe to arrangements with DHS as they do not wish to be confronted with data which might compromise "visa overstayers" within their own community (cf. Koslowski, 2007).

---

[17] Council Regulation (EC) No 539/2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement as last amended by Council Regulation (EC) No 851/2005 of 2 June 2005, OJ L 141, p. 3 of4.6.2005

[18] ICAO Doc 9303, Part 1 Machine-Readable Passports

[19] Complete name; date of birth; place of birth; gender; country of citizenship; passport number and country of issuance; country of residence; travel document type (e.g., visa), number, date of issuance, country of issuance, issuing country code, and expiration date; complete U.S. address; arrival and departure information; digital photograph; fingerprints; encounter data (DHS US-VISIT 2007)

[20] For complete information on the standards see http://www.itl.nist.gov/div893/biometrics/standards.html

[21] "ten fingerprints taken flat and digitally captured"; cf. COM(2006)269 final, http://www.statewatch.org/news/2006/jun/COM-2006-269.pdf

[22] For the complete list of authorities with possible access authorization according to DHS US-VISIT, see Annex 2

The **VIS** package, on the other hand, bears the mark of the delicate compromise achieved. When in the years after 2001, the option of interlinking the various EU large-scale IT-systems (SIS II, Eurodac, VIS) was at least theoretically considered (EU Commission, 2005), the concept met with violent opposition by all those that were concerned about scenarios of "function creep", Orwell-like visions of data mining and a "European surveillance society", etc. As a consequence, the new legislation very clearly defines safeguards against any uncontrolled diffusion of this highly sensitive type of data.

Articles 3 and 18-20 VIS-Reg together with Article 7 of VIS-FD make it very clear that VIS is primarily a tool of visa policy and that access by other government branches must remain a closely supervised exception. The sensitivity of the data henceforth contained in the world's largest biometric database and their susceptibility to specific privacy risks in form of profiling and related kinds of processing make it indispensable that police and intelligence authorities will be denied any uncontrolled "on tap" access. The **"filters"** employed by the VIS package are the following:
- a three-tier system of access rights, i.e. visa authorities as the normal "stakeholders" (Art. 2 VIS-Reg), border and other authorities competent to carry out identity checks (Art. 18-20) and finally, with the strictest conditions imposed, authorities, including Europol, competent for the prevention, detection and investigation of terrorist offences and serious crime (Art. 3)
- set of material conditions according to which (1) only the prevention, detection and investigation of serious crime (terrorist offences in the sense of Art. 1 – 4 Council FD 2002/475/JHA[23] or serious criminal offences in the sense of Council FD 2002/584/JHA[24]) qualify for the granting of access (Art. 2.1 (1) and (2) VIS-D07), while (2) the consultation of VIS must not only be necessary for the above purposes but also (3) promise to substantially contribute to these aims (Art. 5 (1) VIS-D07).
- procedural mechanisms
A highly formalised procedure ensures that only designated Member States authorities and Europol (Art. 5 – 7 VIS-D07) are entitled to access VIS and that all consultations take place via the one central access point designated by each Member State (Art. 3 (1b)). Further safeguards include monitoring at all levels (Art. 12(1), 8 (6)), including self-monitoring (Art. 8c).

1.7 System architecture

VIS and US-VISIT are both "embedded" in a wider database landscape designed for the purposes of border/immigration control, law enforcement etc. The relationships are, however, quite different.

US-VISIT as a "system of systems" (DHS 2003) and integrated into an environment of three pre-existing DHS databases (Arrival and Departure Information System ADIS, Passenger Processing Component of the TECS and Automated Biometric Identification System IDENT)[25] has from the start been designed to widely interface with other DHS components such as SEVIS (immigration and customs enforcement) and CLAIMS 3 (US citizenship and immigration services). Further interfaces particularly concern the Department of State's Consular Affairs Consolidated Database (CDD) from which it receives biographic and biometric information as part of the visa application process, and returns fingerscan information and watchlist changes (DHS 2005, p 9). For illustration of the architecture see the flow chart in Annex 1[26].

VIS, although sharing the same technical platform with the SIS II database, has been designed as an entirely separate system without interface to any other large scale IT-system at EU-level such as SIS II and Eurodac. Although in the framework of post-9/11 discussions (see 1.6 above) concepts of synergy and interoperability were examined, privacy considerations finally prevailed to keep VIS entirely apart.

[23] OJ L 164, 22.6.02, p. 3
[24] OJ L 190, 18.7.02, p. 1
[25] DHS (2005), p. 9,10
[26] Individual updates after 2003 can be retrieved from http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm#12

1.8. Data protection and privacy in general

The different significance of privacy concerns in both systems may be illustrated by the respective legal texts which in the case of US-VISIT contain no reference to privacy or similar keywords whereas in VIS legislation provisions on privacy/data protection play a rather dominant role.

The absence of privacy provisions in **US-VISIT** legislation indicates possibly just an issue of transparency, as according to administrative publications as well as explanations by DHS officials, the protection of privacy concerns is taken care of by so-called "System of Records Notices" (SORN) as required by the Privacy Act of 1974 for each data system. The SORN for US-VISIT (as received from DHS upon request) contains provisions on safeguards (mainly of a technical nature), retention and disposal (fixing a retention period of 75 years!) and procedures for record access (whereby it is stated that "The major part of this system is exempted from this requirement").

Although there was no express mention in he SORN, DHS representatives stressed that for the relevant rights/procedures no distinction was made between US citizens (some are listed in US-VISIT!) and foreigners. Due to the scarce information basis available, further research would appear appropriate to identify the exact legal situation of travellers affected by data stored in US-VISIT.

VIS in turn applies considerable care in displaying the comprehensive rules of data protection, notably by means of Art. 7(1) (Principle of necessity, appropriateness and proportionality), Art. 7(2) (non-discrimination), Art. 23 (retention period) Art. 31 (data protection in case of transmission to third countries), Art. 33 (state liability), Art. 37 (right of information), Art. 38 (right of access, correction, deletion) which makes VIS appear fully in line with the standards currently in force in the European Union.

1.9 Data retention periods

As laid down under section 1.8 above, there are considerable divergences as regards the retention periods for data stored. While under **US-VISIT** the maximum period for all electronic records is 75 years (DHS 2006a), VIS limits the retention for data storage to maximum of 5 years (Art. 23 VIS-Reg).

1.10 Entry-exit system

In conformity with its legal mandate, **US-VISIT** has from the very beginning been intended as an "automated entry and exit system" (IIRAR Act 1996), initially in order to identify visa-overstayers. If the combined entry-exit control after more than 10 years still remains in the headlines[27], this has to do with the still not completed exit element, because despite an enormous budget already spent (approx. 1 billion $ by the end of 2005)[28], "our air, sea and land ports lack the infrastructure to conduct such controls" (US-VISIT Director R. Mocny at a hearing in Congress on 28 June 2007[29]).

This appears all the more remarkable since the extraordinary funding invested in US-VISIT was last but not least motivated by a loophole discovered in the aftermath of 9/11, ie that top terrorist Mohamed Atta when entering the US on January 10, 2001 should have been refused entry because he had overstayed a previous visa. But due to uncoordinated database contents, this circumstance remained undetected (Koslowski 2005, p. 8).

It is widely recognized that the US-VISIT system has made remarkable progress towards achieving an integrated system with coordinated biometric controls at both ends. A test phase completed on 7 May 2007 at 14 airports has evidenced that from the technical point view, biometric exit controls pose no problems. Just like at entry, an average of merely 15 seconds have to be added to the processing time (ibid.). The remaining

---

[27] CF HEARING BEFORE THE HOUSE SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL COUNTER TERRORISM ON 28 JUNE 2007, WHICH ALMOST EXCLUSIVELY FOCUSSES ON THIS SUBJECT, DHS (2007A)
HTTP://WWW.DHS.GOV/XNEWS/TESTIMONY/TESTIMONY_1183137626694.SHTM

[28] Koslowski (2005), p. 10

[29] DHS (2007a)

difficulties at airports concern the smooth incorporation of biometric exit controls (automated kiosks) into the airline check-in process. DHS intends to publish a Notice of Proposed Rulemaking before the end of 2007 outlining its plans thereto relating (DHS US-VISIT, 2007).

Headaches at DHS are rather caused by the situation at **land borders** which account for 80% of 430 million persons crossing US border annually (GAO 2006, p. 16). The problems appears dual: on the one hand, land ports of entry (besides "green" and "blue" borders) represent the major loophole in the U.S. border protection (Koslowski 2005, pp. 33,37): almost 99% of these crossings take place outside of the coverage of US-VISIT as they involve US or Canadian citizens anyway exempt from the program as well as Mexicans who on the basis of border crossing cards do equally not require a visa. If, on the other hand, all these entry/exit operations were subjected to simple controls such as showing passports/crossing cards at primary inspection or checking the document against an automatic reader, this would lead to unprecedented traffic congestions.

Improving the infrastructure by the construction of additional lanes and booths, the installation of biometric readers and workstations, and the hiring of inspectors would cost an estimated 2.9 billion $ (ibid p. 39), but not represent a guaranteed solution: passing the controls even at a reduced speed by means of radio-controlled readers (RF-technology) would cause congestions. Currently tests are conducted with biometric readers to carry out biometric controls on cars passing at a speed of 55 mph (=100 km/h) but the outcome is yet uncertain - and so is that of US-VISIT on the whole (see Part 2 below).

VIS again differs considerably from such ambitious aims: although the system has developed from a mere visa-issuing tool as originally projected to one which also serves to other purposes (controls at borders and within the territory as well as asylum and law enforcement), the introduction of an exit-element has not yet been seriously considered. The idea surged only once in the context of the discussion of enhanced synergy and interoperability of EU databases (EU Commission 2005) but was not pursued any further due to reasons of data protection and practicability.

1.11 Practical case study: business processes for (a) an EU citizen travelling for business purposes to the US and vice-versa of (b) a US citizen travelling for business purposes to Europe.

a. Travel to the US

Phase 1: Pre-entry phase (in the country of origin)

Travellers from ***non-VWP countries*** (all Member States except AU,BE,DK,FI,FR,DE, IE,LU,NL,PT,ES,SL,SW,UK) **apply for a visa** at the local US embassy/consulate. This is subject to an appointment which needs to be taken 2 to 14 days in advance (for exact wait times consult http://travel.state.gov/visa/temp/wait/tempvisitors_wait.php). At the appointment, the applicant has to present a completed DS-156 form for a B1 visitor visa, current, valid passport or travel document, 2 photos (size 2x2 inches, evidence of funds to cover expenses in the United States, evidence of compelling social and economic ties abroad, supplemental Nonimmigrant Visa Application, Form DS-157, for men between 16-45 years of age, payment of a nonrefundable US $100 nonimmigrant visa application processing fee. During the interview, an ink-free, **digital fingerprint scan** (2 index fingers) will betaken.
All **data provided are checked** against the Consular Lookout and Support System (CLASS) watch list, which includes data from the Justice Department's National Crime Information Center (NCIC) system, a computerized index of criminal justice information (criminal records, fugitives, terrorist lookouts, missing persons, etc.) as well as other Interagency Border Inspection System (IBIS) watch lists. A **record is then generated within IBIS/IDENT (**system shared by twenty law enforcement and border control agenciesthat resides on the Treasury Enforcement Communication System (TECS) at the CBP Data Center. After the checks the visa application is either approved or denied. Please note: (1) the actual issuance of the visa requires another delay (normally 2 days), and (2) the **visa is just a „permission to apply to enter the United States(!)".**

Travellers from ***VWP countries*** (AU,BE,DK,FI,FR,DE,IE,LU,NL,PT,ES,SL,SW,UK) need to present **machine-readable passports**. In addition, passports issued or renewed/extended on or after 10/26/06 require

integrated chip with information from the data page (e-Passport). If issued or renewed/extended between 10/26/05 and 10/25/06, they require digital photograph printed on the data page or integrated chip with information from the data page. Please note: In the future, VWP travellers need to register travel plans 48 hours in advance in order to obtain an **Electronic Travel Authorization (ETA)!**

When travellers with a B1 visa or under the VWP board a US-bound airplane or ship, the airlines and sea carriers are required to electronically transmit passenger manifests using the **Advance Passenger Information System (APIS)**. Passenger data on these manifests are then checked against watch lists in advance of arrival at US ports-of-entry.

Phase 2: Entry at US port (PoE)

Upon arrival, travel documents are scanned into IBIS. IBIS and APIS queries generate any existing biographical lookout hits and existing records based on manifest data. IBIS also indicates if there are any existing fingerprints in the IDENT database that were submitted during the visa application process. Once a biographical record is generated from the Consolidated Consular Database (CCD) or from passenger manifest data, the inspector switches to the IDENT screen, takes the person's **photograph and scans each index finger**. These biometrics are checked against the IDENT database. If there are no fingerprints in the database, **the person is enrolled in US-VISIT**; if there are fingerprints that were submitted during the visa application process, a one-to-one match with data from the initial enrollment abroad verifies the individual's identity. If there is a watch list hit or a biometric mismatch, the person goes to secondary inspection for additional screening.

Phase 3: Exit at US port (PoE)

Air and sea carriers transmit electronic manifest data through APIS, which is then matched to entry records in ADIS for a corresponding entry-exit confirmation. Departing visitors "check out" of the country at self-serve US-VISIT exit stations either 1) at self-service exit stations, where they place their **two index fingers on the scanner, have a digital photograph taken**, and receive a printed receipt that verifies checkout; or 2) at the departure gate by a US-VISIT attendant using a portable biometric reader/exit processing device. IDENT then executes a **one-to-one match comparing the exit to the entry record**.
In the (rare) case of exiting via a land port, the traveller submits an I-94 arrival departure record.

b. Travel of US citizen to EU-Schengen countries

US citizens travelling to EU-Schengen countries are **exempt from any visa requirements** for short-term stays up to 90 days[30].

2. Current developments as regards the US-Visit system

US-VISIT is currently struggling at various fronts to close remaining security gaps while trying to preserve freedom of travel to the utmost degree possible.

2.1 Extension of entry-exit element to land borders

While security gaps have been widely closed at air and sea ports of entry, the land borders remain a great concern. Different from air and sea entries, these ports are hardly used by long-distance travellers but rather by those who cross the border in a daily routine and in great numbers. Consequently, the possible introduction of US-VISIT formalities – even if confined to minimum delays of 10-15 seconds per passenger – would lead to unprecedented **traffic congestions**.

Land borders accounting for approx. 80% of all cross-border traffic represent the **most important loophole in US border protection** (Koslowski 2005): on the one side, the enormous volume of approx. 330 million visa and US-VISIT-exempt travellers per year (US and Canadian citizens, Mexican citizens with border crossing cards) present a perfect environment for unwanted foreigners (terrorist or others) to enter the US

[30] cf Council Regulation (EC) No 539/2001 as amended, see Fn 15 above

unrecognised and via official ports of entry. On the other side, the border line away from official ports of entry ("green" or "blue" borders, especially the lakes and rivers between Canada and US) offer ideal opportunities for illicit crossings, especially if one mixes with Michigan's thousands of recreational boaters on Detroit River (Koslowski 2005, p. 23).

The congestion problem at land ports of entry may be resolved even it is at the expense of huge investments, but no solution is in sight for the green/blue border issue. As experience shows, even hi-tech border devices such as along the US-Mexican border remain vulnerable.

2.2 **Transition to 10-Fingerprint Collection at Borders**

According to DHS, the transition to the collection of 10-Fingerprints has already started at US embassies and consulates around the world and will be introduced at 10 US airports later this year. The new system is expected to work as rapidly as the previous collection of 2-fingerprints while providing a greater security in avoiding mismatches[31]

2.3 **Electronic Travel Authorization (ETA)**

The ETA concept as copied from the Australian model in force since 1996 offers to US authorities the advantage of an advance check of all incoming travellers; however, with the **requirement for travellers to notify travel plans 48-hours in advance**, this control mode risks to become highly unpopular with all business travellers who prefer to take travel decisions at the last moment. Combined with other complications already imposed on travel to US destinations, recent media reports assume that this will reinforce the trend already observed among multi-national companies to hold business meetings and conventions outside the U.S.[32]. The same seems to apply to tourist travel, as Member States observe a strong reduction of tourist travel flows to the US[33]

2.4 Related areas: New PNR agreement and VWP modernisation

The new **PNR agreement concluded on 29 June 2007** at the intergovernmental level allows EU airlines to continue to serve US destinations after the expiry of the current interim agreement. Critics such as EDPS Peter Hustinx express a number of grave concerns on the content of the new instrument from the privacy point of view, ie (1) the data retention period raised from 3.5 to 15 years (by means of the "dormant" data concept), (2) accessibility of the data by a wide range of US authorities without limitations being imposed as to the intended use, (3) absence of robust legal mechanism for EU citizens in case of abuse, and (4) avoidance of a binding agreement via exchange of letters, (5) despite the reduction from 34 to 19 data fields to be completed, the content remains about the same due to rearrangement of questions [34].

According to DHS Secretary Chertoff, changes intended by the modernised **Visa Waiver Program (VWP)** would include the following:
- electronic travel authorization ETA (see 2.2 above)
- enhanced passenger information exchange
- prompt reporting of lost/stolen passports
- introduction of common standards for travel documents
- air marshals
- superior standards for airport security.

It is emphasized that the revised program would facilitate the joining of VWP by EU Member States mainly in eastern Europe so far not admitted.[35]

---

[31] P.T. Wright, Acting Deputy Director of US-VISIT at a Press Conference in Brussels on 25 June 2007, http://useu.usmission.gov/Dossiers/Travel_Documents/Jun2507_Wright_US-VISIT.asp
[32] Internat ional Herald Tribune of 15 June 2007, US proposals raise fears in Europe.
[33] FDP Enquiry in the German Bundestag 16/5666 of 13 June 2007
[34] Letter to Dr. Schäuble, Chairman of EU JHA Council, of 27 June 2007, http://www.statewatch.org/news/2007/jun/eu-us-pnr-hustinx-letter.pdf
[35] statement of 1 December 2006, http://usinfo.state.gov/utils/printpage.html

Conclusions

The comparison has confirmed the old saying that outer appearances may greatly mislead: despite striking similarities in name, VIS and US-VISIT are essentially different in design as well as general orientation. Although the differences established correspond to a transatlantic divide in political priorities (protection against terrorism vs support of the common visa system and ,in particular, prevention of visa shopping), one should not ignore certain temptations on EU-side to pursue parallels beyond the existing limits. “Threats to internal security”, although currently just a subordinated motive, may climb up the ladder of importance in view of extraordinary incidents/events and secondly, even within existing border-related concerns, one might consider to perfect the existing devices by introducing a biometry-based exit element[36].

For Europeans, it is well to recall the outcome that perfectionist concepts have so far encountered in the U.S.: despite stringent rules and enormous investments, the border line is far from becoming an insurmountable obstacle to immigrants and even less to skilled and well-equipped terrorists.

Closing the remaining gaps along the border line, be it across lonely deserts, waters, forests, or at busy ports overcrowded with commuters will cost an disproportionate amount of investment in financial as well as social terms. Citizens should know what they subscribe to in terms of own sacrifices – “to wait longer at inspections, pay more for international travel and submit biometrics for more secure travel documents” (Koslowski 2005, p. 63). All this should be taken into account when preparing decisions, in the US as well as in Europe – instead of making people believe that technology will do it all and there will be little if any impact on their lives and pocketbooks.

[36] e.g. by taking up one of the scenarios developped in theory by Commission communication COM(2005) 597 final which includes the “long-term scenario” of an entry – exit system (cf EU Commission 2005, section 5.3, p. 7ff)

Bibliography

DHS (2003), US-VISIT Program, Increment 1 Privacy Impact Assessment, December 18, retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_inc1.pdf

DHS (2005), Privacy Impact Assessment Update for the US-VISIT Program In Conjunction with the Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Ports of Entry, July 1, retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisitupd1.pdf

DHS (2006), US-VISIT Enrollment Requirements, retrieved from http://www.dhs.gov/xtrvlsec/programs/editorial_0527.shtm

DHS (2006a), System of records notice. US-VISIT - ABIS/IDENT, July 27, retrieved from http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/E6-11995.htm

DHS (2007), US-VISIT: How It Works, retrieved from http://www.dhs.gov/xtrvlsec/programs/editorial_0525.shtm

DHS (2007a), Joint Statement for the Record, Robert A. Mocny Director US-VISIT Program And Robert Jacksta Executive Director Traveler Security and Facilitation Office of Field Operations U.S. Customs and Border Protection Before the House Subcommittee on Border, Maritime, and Global Counter Terrorism, June 28, 2007, retrieved from http://www.dhs.gov/xnews/testimony/testimony_1183137626694.shtm

DHS US-VISIT (2005), Privacy Impa ct Assessment Update for the US-VISIT Program, Washington D.C., July 1, 2005, retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisitupd1.pdf

DHS US-VISIT (2007), Responses to question list by Peter Hobbing, as transmitted by e-mail on 2 July 2007

EU Commission (2005), Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, Brussels, 24.11.2005

EU Council of Ministers (2001), Conclusions adopted by the Council (Justice and Home Affairs) Brussels, 20 September, Doc. SN 3926/6/01 REV 6

GAO (2006), Report to Congressional Requesters on BORDER SECURITY. US-VISIT Program Faces Strategic, Operational, and Technological Challenges at LandPorts of Entry, GAO-07-248, December 2006

Hayes, B., *From the Schengen Information System to SIS II and the Visa Information System (VIS): The proposals explained*, Statewatch Report, February 2004.

Koslowski, Rey (2005), Real challenges for virtual borders. The Implementation of US-VISIT, Migration Policy Institute, Washington D.C.

Ludford, S. (2007), "Defending data", ParliamentMagazine of 4 June 2007, p. 15

US-DoS (2006), Visa Waiver Program (VWP), retrieved from http://travel.state.gov/visa/temp/without/without_1990.html

van Herpen, M. (2004), „Six Dimensions of the Growing Transatlantic Divide: Are the US and Europe Definitively Driving Themselves Apart?", in: Hall Gardner (Ed.), *NATO and the European Union – New World, New Europe, New Threats*, Aldershot (Ashgate), retrieved from: http://www.cicerofoundation.org/pdf/ chapter_vanherpen.pdf

Interviews (conducted by phone/e-mail)

Rey Koslowski, Associate Professor of Political Science and Public Policy, University at Albany (SUNY) Director of research project on "International Migration, Border Control and Homeland Security in the Information Age," (26 June 2007)

Robert Mocny , Director US-VISIT (27 June 2007)

Steve Yonkers, Acting Deputy Assistant Director US-VISIT (29 June 2007)

Karyn Becker, Privacy Analyst US-VISIT (28 June and 2 July 2007)

Legislation

1. EU

VIS-D04 2004/512/EC:Council Decision of 8 June 2004 establishing the Visa Information System (VIS) OJ L 213 , 15/06/2004 P. 0005 - 0007

VIS-D07 Council decision .../2007/JHA of ... concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, retrieved from http://www.europarl.europa.eu/sides/getDoc.do?Type=TA&Reference=P6-TA-2007-0229&language=EN

VIS-Reg Regulation No .../2007 of the European Parliament and of the Council on the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, adopted on 14 June 2007, http://www.europarl.europa.eu/sides/getDoc.do?Type=TA&Reference=P6-TA-2007-0227&language=EN

2. US

IIRIR Act (1996): Illegal Immigration Reform and Immigrant Responsibility Act of 30 September 1996, (Public Law 104-208), retrieved from http://www.lib.umich.edu/govdocs/text/104208.txt

DMIA Act (2000): Immigration and Naturalization Service Data Management Improvement Act of June 15, 2000, (Public Law 106–215), retrieved from http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename= publ215.pdf&directory=/disk3/wais/data/106_cong_public_laws

USA PATRIOT Act (2001): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 26 October 2001, (Public Law 107-56), 115 Stat. 272 (2001), retrieved from http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=publ056.pdf&directory=/diskc/wais/data/107_cong_public_laws

EBSVER Act (2002): Enhanced Border Security and Visa Entry Reform Act of 14 May 2002, (Public Law 107–173), retrieved from http://www.gpoaccess.gov/serialset/creports/pdf/108-796/conference_contents.pdf

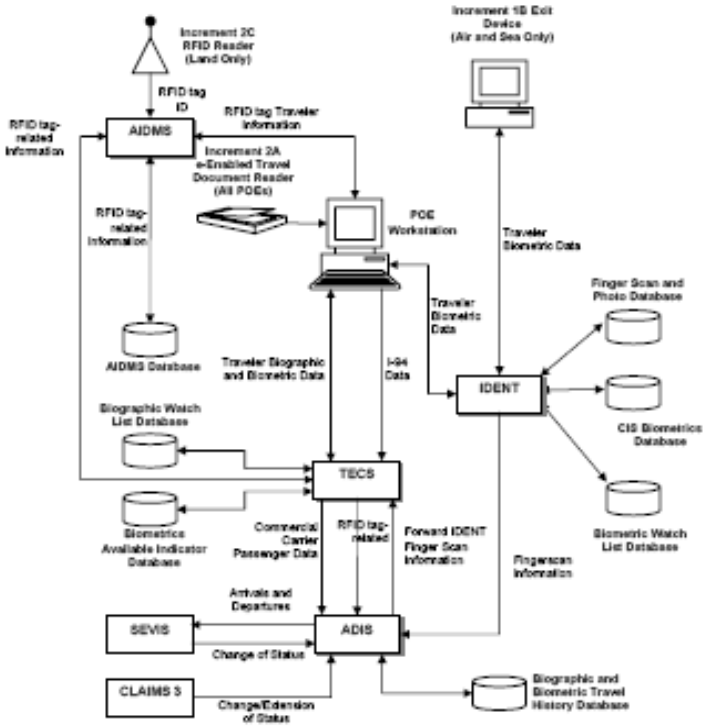
IRTP Act (2004): **Intelligence Reform and Terrorism Prevention Act** of 12 July 2004; (Public Law 108–458), retrieved from http://www.nctc.gov/docs/pl108_458.pdf

Abbreviations

FD	Framework decision
GAO	United States Government Accountability Office
ICAO	International Civil Aviation Organization
SORN	System of records notice
US-DOS	U.S. Department of State
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
VIS-D04	2004/512/EC: Council Decision of 8 June 2004 establishing the Visa Information System (VIS)
VIS-D07	Council decision .../2007/JHA of ... concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences
VIS-Reg	Regulation No .../2007 of the European Parliament and of the Council on the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, adopted on 14 June 2007,
VWP	Visa Waiver Program

Annex 1: The US-VISIT architecture

Figure 1: US-VISIT Architecture



Annex 2

List of US authorities with possible access to the information in US-VISIT databases (as communicated by DHS US-VISIT on 2 July 2007)

Authorities with Access: The following is a list of authorities with possible access to the information maintained in US-VISIT databases. [This is not carte blanche access. Other controlling factors may include data access controls, need-to-know and existence of Memoranda of Understanding.]

A. To appropriate Federal, state, local, tribal, foreign, or international Governmental agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest, for purpose related to administering or enforcing the law, national security, immigration, or intelligence, where consistent with a DHS mission-related function as determined by DHS.

B. To appropriate Federal, state, local, tribal, foreign, or international government agencies charged with national security, law enforcement, immigration, intelligence, or other DHS mission-related functions in connection with the hiring or retention by such an agency of an employee, the issuance of a security clearance, the reporting of an investigation of such an employee, the letting of a contract, or the issuance of a license, grant, loan, or other benefit by the requesting agency.

C. To an actual or potential party or to his or her attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, or discovery proceedings.

D. To a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains.

E. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. Sections 2904 and 2906.

F. To individuals who are obligors or representatives of obligors of bonds posted.

G. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish a DHS mission function related to this system of records.