UK: e-Borders plan to tackle “threats”

The scheme is one of the most advanced in the world - but will not be fuly in place until at least 2018

When it comes to border controls the UK is going to be way ahead of both the EU and the USA. Whereas in the USA plans for introducing profiling system (CAPPS II) for all passengers was withdrawn after a damning report from the General Accountability Office (GAO) and opposition from civil liberties groups. It is being replaced by a straightforward watch-list monitoring programme, that is, checking all passengers against a list of around 125,000 people. So far in the EU plans were agreed in April 2004 for the mandatory collection of passenger name records (PNR) and for biometrics (eg: finger-prints) in visas and passports (introducing fingerprints on EU ID cards is planned). But there is, as yet, no overall plan for how each of the 25 member states will use the data collected.

The UK's "e-Borders Programme" is intended to be a comprehensive system with the mandatory collection of data and biometrics for everyone who enters and leaves the country.

It will build on new powers in the Immigration and Nationality Bill currently before parliament and some of its implications are given in a "Partial Regulatory Impact Assessment on data capture and sharing powers for the border agencies" (RIA).

Scope and objectives

Once in place the UK's "e-Borders" system will be with us for evermore and the original, legitimating purposes, terrorism and organised crime in this case, can grow exponentially. As the police purposes in the RIA spell, the system is not just need for "terrorism and organised crime" but "to support general police and criminal justice functions" (p35).

The overall "Objectives" are set out as:

1. the "ability to deny travel"

2. "assessing in advance of arrival [of] the immigration and security threats posed by passengers"

3. to share information between immigration, police, security and intelligence agencies

4. to use "passenger information" and intelligence to inform the agencies.

The agencies will "capture" passenger data through a "single window" and jointly analyse "bulk data" and retain the data for an indefinite period.

The immigration, police and security agencies already have powers to require carriers (air, sea and land) to provide information of people travelling to the UK and "in some cases" from the UK (ie: to the USA).

However, the decision to "share or disclose information must be considered on a "case-by-case" basis" where the agencies can rely on "certain information processing exemptions" under the 1988 Data Protection Act "but again, this is on a "case-by-case" basis". Nowhere is it spelt out how data protection is going to work when the agencies "hoover-up" the data on every movement, add comments to some entries, or pass it to any foreign law enforcement agency (as provided for in the Bill).

The e-Borders programme will be delivered in three stages between 2004-2014 and include the "Iris Recognition Immigration System" for automated entry controls using biometrics, the e-Borders Operations Centre (e-BOC) authorising "Authority to Carry" which will "roll out incrementally to all air, sea and rail carriers operating internationally to/from all major UK ports".

The shift in logic is explained as follows. They are many "key drivers influencing the development of the e-Borders proposal" so in responding to these "drivers":

e-Borders seeks to move away from targeted use of the agencies' passenger information powers, towards the routine and comprehensive capture of data, underpinned by the "single-window" facility for carriers to provide passenger information to Government.

Or put another way, instead of targeting suspects information and data will be "captured" on everyone entering or leaving the UK.

Current statutory powers allow agencies to share information to "fulfil their own individual statutory functions", but:

They do not envisage the Border Agencies participating in joint activities for the greater corporate good, including the joint analysis of carrier data to enhance border security in the wake of the prevailing levels of threat to UK homeland security.

The "capture", sharing and analysis of passenger data is:

is not confined to a single journey. In this respect, it is essential that law enforcement and intelligence agencies can retain passenger information for a sufficient period of time to achieve the aim of maintaining an effective border security capability... An audit trail of movements which illustrates a passenger's compliance will weigh in that passenger's favour while evidence of non-compliance will clearly attract closer examination by an immigration officer.

It is thus clear that the UK will also set up the equivalent of the US Visit programme which keeps a historical records on all entrants.

Passenger information, or PNR (Passenger Name Record) as it is more widely known, is provided when a person books a ticket. This is to be supplemented by Advanced Passenger Information (API) whereby airlines flying to the UK will have to install passport readers at check-in desks and supply a list of those actually travelling to the agencies. The cost of this may be passed onto passengers by the airlines.

The PNR and API schemes are to be supplemented by the "Authority to carry" (ATC) scheme are "geared to the perceived risk" thus:

"An authority to carry (ATC) scheme will allow the Immigration Service to prevent specified categories of passenger from travelling to the UK by requiring carriers to request a check against government databases before departure.

Profiling and “low risk” passengers

The Border Agencies will make use of profiling which involves running a series of pre-defined profiles against reservation data. Most profiles are based on information obtained from actual results or from intelligence received

Under another new scheme "low risk" passengers will "qualify for faster clearance" which will be open to UK citizens, those permanently or temporarily resident, visa-holders and "frequent visitors who meet certain criteria" for whom:

There will be a one-off enrolment process, for those wishing to use the system. When they subsequently arrive at any of the UK ports with IRIS barriers, they will bypass the queues to see an immigration officer and look into a camera. If the system recognises them as being admissible, a barrier will open automatically and let them into the UK. Use of the IRIS barriers may be extended in the future to holders of biometrically-enabled travel documents, without the need to pre-register.

This logic begs a number of questions. First, if a person is not a suspect then they will pass through the whole system with ease,

both those who do so legitimately and those not known to or being targeted by the agencies. Second, so too will those who have established a false, unblemished, identity. Third, as the "IRIS barriers" become established at all points of entry those who do not have biometric passports or choose not to give the state yet another personal biometric may find their "profile" records this fact. Finally, the whole system depends on "profiles" whose content is undefined and may be extended to new categories depending on the climate of "fear".

"Enhanced powers" for the agencies

New powers are to be given to customs, police and immigration agencies which will make mandatory the provisions of passenger data in advance of arrival for journeys to and from third countries (non-EU) and to and from EU countries by carriers. This will allow:

> *sufficient time for the information to be used for profiling and targeting of individuals of potential interest, and allow time for a decision to be made as to whether an intervention is appropriate*

Targeting is to be directed not just at individuals to record their "patterns of travel" but also at "high risk flights", that is, flights to countries like Pakistan and Saudi Arabia.

The Immigration Service will have extended powers to request additional Advanced Passenger Information (API) biometric data from travel documents and "additional reservation data to the extent that it is known to the carrier" in electronic format.

Checking biometric data on arrival

The EU Directive on passenger information will require carriers to provide this data in advance of departure:

> *an obligation for carriers to transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State*

In the discussions on the Directive the UK led the demand for passenger information to be handed over in advance of departure on a journey to the EU - this is to allow intervening to stop a suspected person travelling.

An amendment in the Immigration and Nationality Bill will:

> *require any arriving passenger to provide information of an external physical characteristic to verify their identity and confirm they are the rightful holder of that document.*

Everyone arriving will be subject to these checks - UK residents, EU residents and non-EU people. The check will involve the taking of a biometric "on the spot" to check against the biometric held on the chip in a travel document.

The new system will develop in a number of stages. Under EU measures all *new* passports issued in the 25 member states have to include a facial image, that is, a digitised image of the normal passport photo by August 2006. All new passports after February 2008 have to hold real biometric finger-prints. As the current norm for EU passports is 10 years it will take until 2016 for all passports to have a facial image (though in the later stages this may well be an image taken with special facial recognition which plots up to 1,820 unique features on a person) and until 2018 for all to carry finger-prints.

The new powers mean that an immigration official will i) access the information held on the "chip" of all those who have chips in their passports/travel documents and ii) check that the data relates to the person presenting the document.

EU nationals and all other third country nationals arriving will be required to "provide biometric information" which can be compared with the information held on the document presented - this will be a "one-to-one" check involving the mandatory taking of a biometric if the travel document contains one. That is until a EU-wide database is set up to conduct "one-to-many" checks.

For British citizens it will mean comparing the biometric information provided against that contained in the passport or "that contained in any future "national identity register"".

UK "roll-out"

The UK's "e-Borders" system will, when implemented, be one of the most comprehensive in the world and potentially the most intrusive. As it rolls out there will be an initial stage (when only a few people have biometric passports starting in the autumn of 2006 or are registered on the IRIS automated entry system), an intermediate stage (in about seven years' time when half the issued passports will have biometric facial images and finger-prints and the take-up on the IRIS automated entry system may well have increased) and the final stage (when all UK residents will, in theory, have biometric passports around about 2018).

So there will, at the intermediate stage, be a number of different queues at border control points:

1. Those using the automated entry IRIS scheme
2. Those with biometric passports/ID cards from the UK (allowing "one-to-one" and "one-to-many" checks) and from other EU countries (allowing "one-to-one" but not "one-to-many" checks until there is an EU-wide database)
3. Those with biometric passports from non-EU countries (allowing "one-to-one" but not "one-to-many" checks)
4. Those with biometric visas issued by the UK/EU (if the "collision" of chips whereby an EU visa chip would clash with a national e-passport chip is resolved; then checked against the Visa Information System, VIS)
5. Those with old-fashion (current) passports from UK/EU
6. Those will old-fashion (current) passports from non-EU countries with biometrically "chipped" visas in their passports *if* third countries agree to this. All that every country is obliged to put in their passports under the ICAO standard (International Civil Aviation Organisation) is simply a digitised image of the usual passport picture inserted onto a readable chip - this is not a biometric and does not require any "enrolment" by the individual.

At the intermediate stage category 5 could constitute 50% of UK and EU passport holders. Or put another way by 2013 around 50% of UK passport holders will have, theoretically, "secure" identities established by biometric checks and 50% will not and the same will be true for EU citizens too. Moreover, the EU is only just starting to think about how to impose finger-printing and the insertion of "EU visa chips" in other nations' passports (category 7).

Patchwork across the EU?

There are many stages in setting up such a system. First, the biometrics have to be collected (through so-called "enrolment") and the biometrics and personal data linked and stored on a central database. Second, "readers" have to be installed at every point of departure (ie: at all check-in desks for all airlines flying to the UK/EU from anywhere in the world). Third, the mass of data has to be checked against "watch-lists" held by the receiving country's agencies and decisions taken on whether to "authorise" travel. Those given a "green" will be able to travel, those given a "yellow" would be subject to extra checks before boarding or placed under surveillance on arrival, and those give a "red" will be refused boarding, be detained or taken into custody. The "yellow" category is the most problematic as this could be because a person is wrongly identified as a potential suspect, as Senator Edward Kennedy was several times before his real identity was established.

It might be thought that having taken the decision in December 2004 to introduce biometrics onto EU passports a standard system for gathering and checking the data would be in

place too, or at least planned. However, it is apparent from a questionnaire sent out from the UK Presidency of the Council of the European Union that a great variety of systems could be in place (Note from UK Presidency: Reading systems for biometric e-Passports at EU border control points, EU doc no: 10559/04, 1.7.05).

When the responses to the questionnaire have been collated there will be a meeting of the Council's Frontiers/False Documents Working Party on 12 October 2005 to which will be invited: “technical representatives from Canada and the United States of America”. Among the questions asked is whether: 1) member states are going to carry out checks at "all border control points, or only selected locations"; 2) "Do you intend reading all e-Passports or just a sample?"; 3) Are you going to carry out "one-to-one checks" or "one-to-many"?; 4) Are you going to carry out "full biometric verification checks" by comparing captured images on the spot or simply display the image stored in the chip for manual comparison? 5) Are you planning for reading e-Passports at other locations, eg: airline check-in?"; 6) Do you have any plans to introduce "automated border control facilities" - for example, through iris scans? 6) does the reading of the machine readable zone automatically link to the Schengen Information System or "your national suspect/warnings database?"

It is clear from the questions that the level of checks and the assumed level of protection from "threats" could vary greatly from EU state to EU state.

What is the point?

The UK e-Borders system will be the first of its kind, and also the first of many. The shift from "targeting" suspected individuals to placing everyone's movements under surveillance raises all kinds of privacy and data protection issues. This is especially as the scope of system which although presented as necessary for countering terrorism and serious organised crime can very easily be extended to cover all crime or all suspected crime however minor.

Equally the "profiling" of an individuals' travel habits or individuals going to or from certain countries raises serious concern that certain groups (eg: young men) and nationalities (northern African, Middle eastern or from Pakistan) will be targeted and subjected to extra checks and surveillance.

The value of the system's product to counter-terrorism is going to be extremely limited for years - biometric checks on less than 50% of those travelling leaves a gaping hole. However, the time scale for the full implementation of the UK, and EU, systems - around or after 2018 - suggest that the scope and use of the biometrics and data collected will have greatly expanded by that time.

This analysis was first published in Statewatch bulletin, vol 15 no 3/4.