statewatch

Analysis

EU: Secretive Frontex Working Group seeks to increase surveillance of travellers

Chris Jones

Frontex has been negotiating in secret to grant state agencies greater access to the personal data of travellers entering the EU. No hard evidence has been presented by EU institutions to support Frontex's claim that this will lead to more effective border management and critics have warned that the mandatory collection of passenger information is entirely unnecessary and a disproportionate infringement of individual privacy.

The EU's border agency Frontex has for the last 18 months been coordinating meetings of a Working Group on Advance Information Challenges for the purpose of "fully exploiting the benefits of using Advance Information (Advance Passenger Information and/or Passenger Name Record) data for improved border management." [1] This boils down to encouraging the greater collection and analysis of personal information from people travelling into the European Union. However, despite significant interest from the law enforcement authorities of EU Member States and other countries, as well as multinational corporations, there is little evidence to suggest that schemes designed to exploit Advance Passenger Information (API) and Passenger Name Record (PNR) information are effective in achieving their stated purposes of separating 'bona fide' from 'illegitimate' travellers. This raises questions over the necessity of further extending systems already in place, particularly because the Working Group's meetings have been sheltered from public scrutiny.

API, PNR and proof

API and PNR data are gathered initially by airline or other travel companies (i.e. rail, maritime) when individuals purchase a ticket or embark on a journey. Originally collected solely for commercial purposes, API and PNR have come to be seen as legitimate targets for state capture and analysis. Governments and corporations have demonstrated an increasing interest in this type of data as part of ongoing efforts to address terrorism, transnational crime, irregular migration, and the illicit trafficking of humans and goods.

Advance Passenger Information [API] consists of the number and type of travel document used, nationality, full names, date of birth, border crossing point of entry into the territory of the Member States, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport, and the initial point of embarkation. Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data mandates the transfer of API from passengers entering EU territory to Member State law enforcement authorities. The Directive was enacted for rather vague counter-terrorism purposes and "in order to combat illegal immigration effectively and to improve border control." [2] EU countries are also obliged to hand API data to Canada [3] although this can sometimes be contained within PNR records and may also be transferred to those countries with which the EU has agreements on PNR data.

There are problems with the EU-wide implementation of the API Directive. It "has not led to a uniform approach between the Member States regarding the information requested from carriers." [4] A Commission study is currently looking into this, with the results expected in autumn this year. Following this, a report to the European Parliament and Council will be drafted "on the operation of the Directive and [will] evaluate the overall impacts and results in each Member State," according to a Commission spokesperson. So far: "no decision on whether to review/adjust the current legislation has been made." Staff at Frontex, however, have clear opinions on legislative adjustments. The agency's 2011 Work Programme notes that:

> *In view of the upcoming… review by the [Commission] of the Directive and in consultation with the [Commission], the need for harmonisation of the requirements used by the Member States that actively use API has been identified. [5]*

This has presented an opportunity to Frontex, which in the same document announces "a series of workshops" focusing on "identifying the future needs for advanced information, while at the same time facilitating the flow of persons crossing the border."

Passenger Name Record (PNR) data is more extensive than API and includes, amongst other things: date of reservation/issue of ticket; date(s) of intended travel; names; frequent flyer information; all available contact information (address, phone number, email); baggage information; travel itinerary; travel status of passenger (including confirmation and check-in status); any collected APIS (Advance Passenger Information System) information; and general remarks, which permits the provision of less standardised information. [6]

The EU currently has agreements requiring flights originating in the EU to transmit this information to the authorities of Australia, Canada, and the USA. The EU is currently discussing its own proposal for a EU-PNR system which will monitor everyone entering or exiting the EU – a majority of Member States are pushing for this to be extended even further to cover travel inside the EU too and, in time, to land, sea and air travel. [7] This would enforce the mandatory surveillance of all forms of transit travelling into and within the EU. Current agreements vary slightly but are all ostensibly geared towards addressing terrorism and serious crime, although the substance of the EU-US agreement in fact goes far beyond this. [8]

There have been heated debates over legislation intended to allow the mandatory collection and analysis of API and PNR data by state agencies, with many considering such practices entirely unnecessary and a disproportionate infringement of individual privacy. Following the parliamentary vote endorsing the EU-US PNR Agreement, Jan Phillip Albrect (a Green MEP) stated that:

> *A majority of MEPs has today voted to reverse the European Parliament's long-standing role in defence of EU citizens' civil liberties and to endorse intrusive big brother style surveillance. Instead of rejecting this senseless and excessive collection and retention of private data, those MEPs who voted in favour of the deal have engaged in gross hypocrisy and sought to wash their hands of the PNR controversy. [9]*

The European Data Protection Supervisor, discussing PNR systems more generally, has noted that:

> *The fact that recent technological developments currently render wide access and analysis possible… is not in itself a justification for the development of a system aimed at the screening of all travellers. In other words: the availability of means should not justify the end. [10]*

No hard evidence has been presented by EU institutions to demonstrate the need for PNR collection and analysis, an omission that certainly raises questions over what is driving border control policy in Europe. The Commission's impact assessment on its proposal for an EU PNR scheme did not contain any statistical evidence, instead it relied on two anecdotes to make its case for the necessity of the system. [11] The Article 29 Working Party, made up of representatives of EU Member States' data protection authorities, has stated that:

> *There are no objective statistics of evidence which clearly show the value of PNR data in the international fight against terrorism and serious transnational crime. [12]*

In light of this, it would appear difficult to explain quite why so many states and institutions are so keen on the further collection and analysis of API and PNR data. Perhaps the most likely reason is that multinational IT and defence firms with an interest in the security industry – a number of which were invited to the most recent meeting of Frontex's Working Group – are seeking new markets, and there is no shortage of politicians anxious to demonstrate to the press and the public that they are "doing something" to protect the populace from all manner of real or imagined threats. One author argues that the growth of the security industry can, at least in part, be explained by the confluence of corporate, political and bureaucratic interests:

> *If marketing is about finding potential customers and then creating demand for your product, the security industry is rapidly becoming a textbook example of how to get rich quick without ever having to test your assumptions… These vested interests are not only a commercial force. Civil servants are more than ever using the fear of terrorism and the need to 'secure' our borders/children/property/energy to further their own interests. [13]*

Frontex and friends

The idea to convene a Working Group on Advance Information Challenges came from Frontex, and the group first met on 17 May 2011 at the agency's headquarters in Warsaw, with representatives from 18 EU Member States' present. The second meeting took place seven months later, on 17 January 2012. The third was held in Brussels over two days, 27 and 28 June. At this meeting representatives from various authorities of 20 EU Member States were present, along with two representatives from the Russian Mission to the EU, staff from two sub-directorates of the European Commission Directorate-General for Home Affairs (border management and return policy and security), and at least one representative of the US Department of Homeland Security. Representatives of data protection authorities have not attended any of the meetings, despite the issues raised by the collection and analysis of API and PNR data by state authorities.

Interested corporations were invited to attend the most recent meeting. The German airline Lufthansa gave a presentation on "Simplifying the Business" on the first day, while the second day was specifically set aside for industry presentations. These came from ARINC, IBM, SITA, Raytheon, Cap Gemini, Morpho and Indra, who were invited for their technological expertise and services in the following fields:

- API/PNR traveller data collection and processing;

- Using traveller data for law enforcement at the border;

- Supporting border management processes/Interoperability of border management systems

Literature produced by some of these corporations elucidates the vision that Frontex and the authorities of many EU Member States have for future systems of border control. ARINC, a US-based subsidiary of the Carlyle Group [14] produces an Advance Passenger Information System currently used by authorities in the Netherlands, Mexico, Costa Rica, El Salvador and numerous other states. The firm recently announced a pilot project with Cyprus "to support evaluation of the use of API as part of enhanced border control in Cyprus." A press release from the company announcing the pilot project quotes Ray Batt, director of ARINC's Government & Security operations: "We strongly believe that the future will demand a continuous increase in the integration of intelligence-led border control systems with advance border control information systems, using Advance Passenger Information (API). The use of API will help increase border security and make the process faster and simpler for the travelling public." [15] Meanwhile, those members of the travelling public who fall foul of "risk profiles" employed by law enforcement authorities are likely to find their journeys far more arduous.

The French firm Capgemini was also present at the meeting. The firm's UK website has an entire section that deals with "border management". Here the company promotes its contracts with the UK Home Office, noting its work to implement iris recognition-based biometric border control, a pilot of the UK's "e-Borders" system. Most crucially for its presence at the Working Group meeting, it also promotes involvement in:

> *[D]e-risking the work involved in data collection from airlines, name matching, watch listing and creating alerts. More recently, we have worked with the UK Border Agency to design its UK Border Force Intelligence Model, helped UKBA and BAA [British Airports Authority] to design an automated clearance system for frequent passengers. [16]*

Frontex agrees that future border control systems will "put additional emphasis on risk-analysis-driven border checks," in particular due to the growth in Registered Traveller Programmes. According to the agency's 2012 Work Programme: "pre-boarding activities, like the analysis of PNR or API, will gain in significance for border controls." [17] The proposed Registered Traveller Programme is, along with proposals for a massive border surveillance system (EUROSUR) and "smart borders", part of a significant attempt to technologically fortify the EU's borders and allow for the sifting of passengers on the basis of automated analysis of information. As one recent study notes, current proposals "would not only infringe fundamental rights, it would also, in spite of its questionable benefits, cost billions." [18]

This has not deterred attempts to introduce these sort of schemes. The UK has undertaken several ambitious technological border control initiatives in the last decade, the most notable being an "e-Borders" system intended to "electronically record every person in the country." The company initially awarded the contract was Raytheon, an invitee at the most recent meeting of Frontex's Working Group. However, following "missed deadlines" and "substandard results" the Home Office terminated its contract with the company. Raytheon launched a lawsuit in response. [19] This is merely one example of many state projects based on advanced technology that have cost more than estimated and taken far longer to develop than intended. As recently as May 2012, the e-Borders project came in for heavy criticism, with a parliamentary committee noting that the system was "highly problematic" and that it "remains concerned about the progress of the e-Borders programme, which has now been undertaken by successive governments." [20] Another notable example is the EU's own second-generation Schengen Information System: "considerably over-budget and with no guarantee of completion." [21]

The UK, it should be noted, is one of a handful of EU Member States whose representatives have been present at every meeting of the Working Group. Staff from the UK Border Agency have also been joined on two occasions by representatives of the Home Office, and once by staff from British Airways. Estonia, Ireland, Germany, Latvia, Sweden, Spain and Poland are the only other states to have been present at all three of the Working Group's meetings. Lists of attendees at all of the Working Group's meetings are contained in the Annex:

http://www.statewatch.org/news/2012/oct/sw-cj-annex.pdf

A closed debate

As noted above, the overall aim of the Working Group is to "bridge the gaps that prevent Member States from fully exploiting the benefits of using Advance Information for improved border management." Improving border management through the use of Advance Information will require significant work, judging by the "key gaps concerning the rollout and operation of Advance Information systems in the EU" identified "according to the input facilitated by the Member States":

- *Lack of technical knowledge and of information on market options for decision-makers*

- *Lack of integration of API with first line border control (both manual and Automated Border Controls)*

- *Lack of integration between API and other information management systems, such as the Visa Information System (VIS)*

- *Unsatisfactory quality of the data transmitted by the airlines and lack of sufficient quality standards and requirements in this respect*

- *Limits to information sharing and absence of risk profiles which are common to the Schengen area*

- *Lack of resources to set up Advance Information Systems*

- *Inaccurate/uncertain perceptions of the costs and benefits of establishing Advance Information Systems*

In order to deal with these problems, it was decided at the Working Group's most recent meeting to set up five sub-groups. Two of these were established by mid-July and a spokesperson for Frontex stated that: "three others will be established during August-September." The sub-groups will deal with the following:

> *- Architecture for Advance Information (AAI): the goal of this Task Group is to develop a reference architecture for a simple but highly effective API system;*
>
> *- Risk Management (RM): it aims to develop best practice guidelines on the setting and operation of a targeting centre; develop best practice guidelines in the analysis of Advance Information; and share risk profiles;*
>
> *- Data Quality (DQ): the objectives are to understand the sources and consequences of insufficient data quality; develop practical criteria for assessing data quality; and identify internal and external best practice guidelines for improving data quality;*
>
> *- Funding (FUN): the goal is to develop best practice guidelines for gaining access to External Border Funds in order to finance the setting up of Advance Information systems;*
>
> *- Costs and Benefits (CBA): this Task Group aims to identify costs/benefits mechanisms and key drivers; and to develop a cost-benefit analysis model*

It is unknown which states and institutions are participating in each sub-group. However, the clear theme that emerges from the "key gaps" identified by and the stated aims of the sub-groups is the need to work more closely with industry in order to produce interoperable systems and the more effective collection and analysis of information. This in turn will permit the subsequent creation of Schengen-wide "risk profiles" in order to establish the criteria upon which it is possible "to verify if the 'profile' of a particular passenger may require a further control by the security services at the borders (or even before take-off)." [22] Such schemes raise questions over privacy, data protection, and the legitimate exercise of state power and should be subject to public scrutiny and debate. Up until now, this has not been the case.

Pushing the boundaries

The first public mention of the Advance Working Group on Information Challenges appeared on Frontex's website at the end of May, in an announcement geared towards the border control industry. A number of documents in the last two years have also hinted at the work being undertaken in the field of Advance Information. The Frontex 2011 Work Programme stated the following:

> *In the successful approach from the previous year for the development of best practices and guidelines will be further developed [sic], now regarding Advance Passenger Information (API). In 2011 the European Commission will undertake a review of the API Directive for which an input on best practices and guidelines would be of great importance. At the same time new ideas regarding API could be introduced. [23]*

It was in this Work Programme that the intention to host "a series of workshops", noted earlier, was announced. In the General Report for 2011, in reviewing the work undertaken by Frontex in that year the agency briefly summarised the project:

> *A project aimed at improving knowledge about the possible contribution of advance information (AI) to border control, specifically towards passenger facilitation and more cost effective risk management. The project covered three distinct specific objectives: current use of AI, challenges and areas for improvement, and best practice guidelines. [24]*

What this demonstrates is that Frontex has pushed its mandate to the limit, if not overstepped its bounds. The legislation applying to the agency until November 2011 permitted it only to "follow up on the developments in research relevant for the control and surveillance of external borders." When amendments to the legislation were finally passed in November 2011, the agency was then able to "proactively monitor and contribute to the developments in research relevant for the control and surveillance of external borders." This raises questions over whether prior to the enactment of the most recent amendments to legislation, the agency was going beyond the bounds of simply "following up on developments in research." The boundary between this and influencing policy-making seems rather blurred, a problem identified in a 2009 study into the role of the EU's decentralised agencies which stated that:

> *Many agencies take a proactive part in shaping new policy issues and raising awareness of these issues among policy-makers, interest groups, and the wider public. In doing so, they play a political role, but this role is always left implicit by [those interviewed for the study] who seem to comply with the institutional division of responsibilities… The evaluation team considers it regrettable that these risks are not acknowledged in an explicit way and addressed as a governance issue. [25]*

The "US perspective"

While Frontex may have convened the Working Group there is no doubt that pressure to increase the use of advance information comes from a number of sources. The United States is a notable example. The Department of Homeland Security (DHS) sent at least one representative to the Working Group's most recent meeting, with a presentation made to the group on the first day covering "the US perspective." Despite repeated requests by Statewatch to the DHS for clarification on their role in the Working Group, they have refused to respond. Clues as to the interest of the US in encouraging border control systems based on advance information systems can however be found elsewhere.

Cables sent by US embassies across the EU in 2009 and 2010, released by Wikileaks, show that there has been significant questioning of European officials and diplomats over their states' role in establishing and advocating advance information-based border control systems. A cable from the US embassy in Bucharest, for example, states that officials from the Romanian Ministry of Foreign Affairs "commented explicitly that the United States could count on Romanian political support at the EU level for ratification of...the [EU-US] PNR agreement." [26] The US embassy in Lisbon noted with regard to both the Terrorist Finance Tracking Program and the EU-US PNR system that "we expect Portugal to make good on its pledge to work with other EU Member States to prevent and combat terrorism at the international level," [27] wording which would seem to indicate that the pledge was perhaps not made just to the EU and its Member States.

US interest in the proposal for an EU PNR, which would permit the collection and analysis of data on passengers flying (and possibly travelling by rail or sea) into the EU, is stark. A cable outlining a meeting between DHS Secretary Janet Napolitano and the EU's Justice and Home Affairs ministers in February 2009 notes that:

> *Ministers of many of the 33 European countries also addressed the plenary, most in support of increased cooperation with the United States, as the Secretary outlined. A primary subject of conversation, however, became the consensus toward establishment of an EU PNR*

> *collection and analysis capability. UK officials later confirmed that they, Spain, France, and others had cooperated before the plenary to achieve consensus on the idea. Denmark, Estonia, France, Germany, Spain, the Netherlands, Portugal, Slovenia, and the UK all spoke in favour. None opposed outright, although Belgium (and Slovenia, to a lesser degree) sounded notes of caution. [28]*

Whether there is consensus amongst the populations of those countries on the idea of an EU PNR scheme remains unknown because no citizens have yet been asked whether they approve of the idea.

Not all EU Member States agree entirely with the aims of US-EU cooperation. Following an October 2009 meeting with Germany's Federal Justice Minister, Sabine Leutheusser-Schnarrenberger, the Berlin embassy noted that they "expect Leutheusser-Schnarrenberger's emphasis on data protection to complicate US government security cooperation both bilaterally and with the European Union." [29] Despite these problems, the US has significant influence over EU security policy and its invitation to the most recent Working Group meeting will have provided aother opportunity to make its views known.

Future of the Working Group

With sub-groups either already in existence or in the process of being established, the Working Group seems set to undertake a significant amount of work and potentially find itself in a strong position to influence future developments in border control policy with relation to the use of advance information. Frontex's 2012 Work Programme notes that despite every EU Member State implementing the API Directive:

> *The roll out of API systems is very limited and heterogenous. Around 50% of MSs do not have an API system in place, and even if it exists, it is seldom used for vessel or railway traffic. This leaves a worrisome open back door for persons trying to enter the Schengen area without fulfilling all the entry requirements. [30]*

These comments, and discussions leading up to the proposal for an EU PNR system, would indicate a significant interest in establishing systems that would enable the systematic surveillance and assessment – based on "risk profiles" drawn up in secret – of all passengers entering, and possibly travelling within, the EU. Considering the intrusive nature of such schemes, the fact that their usefulness is highly questionable, and the involvement of numerous unaccountable individuals, institutions, and third states, the need for greater discussion over and scrutiny of both the Working Group and the subject matter with which it is concerned is urgent. In 2005, in a report on a proposed API and PNR agreement between the EU and Canada, the European Parliament noted that the collection and analysis of such data by law enforcement authorities could open the way for a mass surveillance system and that there was a serious risk of violating the data protection principles enshrined in Article 286 of the Treaty Establishing the European Community, in the Directive 95/46/EC and in the Article 8 of the European Convention on Human Rights and Article 7 and 8 of the Charter of Fundamental Rights of the European Union. [31]

Endnotes

1. http://www.frontex.europa.eu/news/advance-passenger-information-and-passenger-name-record-invitation-for-industry-uQB0Ul

2. http://www.statewatch.org/news/2004/sep/eu-pnr-directive.pdf, Article 3; preamble paras. (1), (2), (3)

3. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:082:0015:0019:EN:PDF

4. http://www.statewatch.org/news/2011/jan/eu-frontex-2011-work-programme-5691-11.pdf, p.57

5. http://www.statewatch.org/news/2011/jan/eu-frontex-2011-work-programme-5691-11.pdf, p.57

6. http://www.statewatch.org/analyses/no-169-eu-pnr-us-aus-comparison.pdf, p.1 and footnote 1

7. 'EU-PNR: Proposals for an EU PNR scheme under discussion', Statewatch News Online, April 2012,

http://database.statewatch.org/article.asp?aid=31446

9. http://www.statewatch.org/analyses/no-169-eu-pnr-us-aus-comparison.pdf

9. http://www.greens-efa.eu/pnr-data-protection-6920.html

10. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-10-19_PNR_EN.pdf, p.4

11. http://www.statewatch.org/news/2011/feb/eu-com-eu-pnr-ia-sec-132-11.pdf, p.12

12. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf, p.3

13. http://www.independent.co.uk/opinion/commentators/nick-pickles-the-security-industry-has-politicians-in-its-thrall-7944310.html

14. http://www.powerbase.info/index.php/Carlyle_Group

15. http://www.arinc.com/news/2012/04-03-12_apis.html

16. http://www.uk.capgemini.com/services-and-solutions/by-industry/public/solutions/justice/border-management/

17. http://www.statewatch.org/news/2012/jan/eu-frontex-2012-wp.pdf, p.16

18. http://www.statewatch.org/news/2012/jun/borderline.pdf, p.5

19. http://www.guardian.co.uk/uk/2011/aug/25/government-legal-action-e-border

20. http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/news/120529-perm-sec-published/

21. http://www.statewatch.org/news/2011/aug/01eu-vis-sis.htm

22. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0226+0+DOC+PDF+V0//EN,p. 7

23. http://www.statewatch.org/news/2011/jan/eu-frontex-2011-work-programme-5691-11.pdf, p.56

24. http://www.statewatch.org/observatories_files/frontex_observatory/General_Report_2011.pdf, p.56

25. http://www.statewatch.org/news/2012/apr/evaluation-eu-agencies-vol-I.pdf, p.31

26. http://cablesearch.org/cable/view.php?id=10BUCHAREST81

27. http://cablesearch.org/cable/view.php?id=10LISBON75

28. http://cablesearch.org/cable/view.php?id=10MADRID190

29. http://cablesearch.org/cable/view.php?id=09BERLIN1377

30. http://www.statewatch.org/news/2012/jan/eu-frontex-2012-wp.pdf, p.16

31. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0226+0+DOC+PDF+V0//EN, p.8

This article was first published in Statewatch journal volume 22 no 2/3, October 2012

© Statewatch ISSN 1756-851X. Personal usage as private individuals/"fair dealing" is allowed. We also welcome links to material on our site. Usage by those working for organisations is allowed only if the organisation holds an appropriate licence from the relevant reprographic rights organisation (eg: Copyright Licensing Agency in the UK) with such usage being subject to the terms and conditions of that licence and to local copyright law.