



Analysis

Commission proposals on migration and internal security databases: a new list of old “needs”

Chris Jones

April 2016

The Commission’s proposal to extend the fingerprinting of short-stay visa applicants to children from the ages of 6 and up is part of a list of possible “enhanced functionalities” (i.e. expanded uses) of the Visa Information System (VIS). [1] These “functionalities” will be examined as part of a larger process of trying to beef up EU and national databases and information systems.

In a Communication entitled ‘Stronger and Smarter Information Systems for Borders and Security’ the Commission sets out its plans for more gathering, exchange and processing of personal data, particularly the data of non-EU nationals. [2] The Commission’s long-term plans are extremely similar to those proposed recently by the German Federal Ministry of the Interior (see further below).

The Communication opens by noting the scale of movement into and out of the Schengen area: its external borders were crossed more than 200 million times in 2015, by “more than 50 million non-EU nationals”. It moves on to conflate refugees with terrorism and to insist upon “the need to join up and strengthen the EU’s border management, migration and security cooperation frameworks and information tools in a comprehensive manner.”

It sets out the intention to amend laws governing numerous systems:

- the Schengen Information System, “to further enhance its functionality”;
- Advance Passenger Information (API, largely made up of biographical information from passports and gathered from air and other passengers entering the EU);
- “The Commission will examine if there is a need to reconsider the legal framework for law enforcement access to VIS and EURODAC,” in the latter case “to further enhance its functionalities as regards irregular migration and return”; and

[1] EU calls for the fingerprinting of 6-year-old children, *Statewatch News Online*, April 2016, <http://statewatch.org/news/2016/apr/fingerprinting-children-visas.htm>

[2] European Commission, Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, 6 April 2016, <http://statewatch.org/news/2016/apr/eu-com-info-smart-borders-int-sec-comication.pdf>

- the European Criminal Records Information System (ECRIS): “to enable national authorities to search for third-country nationals in ECRIS on the basis of fingerprints,” a process that is well underway. [3]

The upgrade of the SIS that will allow it to include fingerprints will be completed. Member States will be called upon to increase their connections to and use of supranational databases (for example, Interpol’s Stolen and Lost Travel Documents or SLTD system) and to get on with networking national ones (the Commission will “launch infringement proceedings against Member States that have not connected to the Prüm framework”). Europol is to make better use of its existing systems and to explore “synergies” between them and others, including the fingerprints to be stored in the SIS.

Zombie ideas: old proposals revived

A central access point to police databases across the EU is to be revived with the European Police Records Information System (EPRIS). The infrastructure for this has in any case been under development as part of the Automated Data Exchange Platform (ADEP) project. [4]

A new proposal has been published for the Entry-Exit System (EES, to gather biographic and biometric data on all non-EU nationals entering the Schengen area), although there is no mention of the Registered Traveller Programme, previously considered a necessary counterpart to the EES. [5]

The possibility of an “EU Travel Information and Authorisation Scheme” for visa-exempt persons is also mooted. It seems this would essentially be a European equivalent of the US Electronic System for Travel Authorisation (ESTA). This proposal has been raised before, as have many of the others – and they will all require “synergies and convergence between information systems and their corresponding infrastructures.”

Join the pots

As the German interior minister, Thomas de Maizière, put it recently: “There has to be a connection of the data pots.” [6]

One could be forgiven for developing a feeling of déjà vu: the Commission’s latest Communication is simply the latest in a series of calls for “interoperability”, a policy favoured since at least 2004 [7] and which often plays a part in propelling the mania for more fingerprinting, surveillance and data capture and processing for “security” purposes.

[3] Council of the EU, Amendments in the ECRIS proposal on the basis of the “consolidated” text following the COPEN (ECRIS) meetings of 1 and 22 February and 1 - 2 March, 2016, 7172/16, <http://statewatch.org/news/2016/apr/eu-council-ECRIS-amendments-7298-16.pdf>

[4] EU: Member States and Europol seek to ease EU-wide access to police databases through “automation of the data exchange process”, *Statewatch News Online*, February 2013, <http://database.statewatch.org/article.asp?aid=32151>

[5] See: Council of the EU, Smart Borders Package –Wrap-up of discussions, 15024/15, 10 December 2015, <http://statewatch.org/news/2015/dec/eu-council-smart-borders-wrap-up-discussion-15024-15.pdf>; for a detailed analysis of previous proposals (including the RTP) see: EU: SMART BORDERS: European Parliament study, *Statewatch News Online*, October 2013, <http://database.statewatch.org/article.asp?aid=32829>

[6] „Gleiche Rechte und Pflichten für alle Ausländer“, *Der Tagesspiegel*, 3 April 2016, <http://www.tagesspiegel.de/politik/thomas-de-maiziere-im-interview-gleiche-rechte-und-pflichten-fuer-alle-auslaender/13394886.html>

[7] EU: The “principle of availability” takes over from the “notion of privacy”: what price data protection?, *Statewatch Bulletin*, vol 14 no 6, November-December 2004,

The development and interconnection of national and EU policing and migration databases has trundled on steadily since “interoperability” first appeared on the scene, amongst other things through giving police forces access to the Visa Information System and to asylum-seekers’ fingerprints in Eurodac; [8] and the automatic transmission to the police of personal data from all plane passengers in the EU (the PNR Directive, due to be implemented soon). [9] Attempts to ensure police access to the EES have been ongoing since the original proposal for the system was introduced in 2013. [10]

“Experts” in the driving seat

This time the Commission wants to provide extra propulsion by setting up an ‘Expert Group on Information Systems and Interoperability.’ According to the Communication, the group will:

“address the legal, technical and operational aspects of the different options to achieve interoperability of information systems, including the necessity, technical feasibility and proportionality of available options and their data protection implications.”

It will also “take a broad and comprehensive perspective on border management and law enforcement, taking account also of the customs authorities’ roles, responsibilities and systems in this respect.”

The group is yet to be assembled. A Commission spokesperson said that: “We cannot at this stage give you more information on the participants.”

One database to rule them all

The Commission proposes a “modular” structure for European information systems, in which different sets of data are connected and accessible to those with access rights through a central “hub”. Different systems should then be directly connected to one another, with “appropriate data protection safeguards and strict access control rules.” A shared Biometric Matching Service (BMS) for the collection and processing of biometric data within and amongst the systems should follow.

The central hub, providing a “single search facility”, “can also be used with mobile equipment,” notes the Commission. While the Communication focuses on policing and migration (and, tangentially, customs) databases, it should be noted that the EU is also encouraging the deployment of fingerprinting for more general purposes. For example, one EU-funded security research project, INGRESS, hopes to “democratise” fingerprinting by making it easier to take

<http://www.statewatch.org/subscriber/protected/sw14n6.pdf>; European Commission, Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, 24 November 2005,

<http://www.statewatch.org/news/2013/jul/eu-database-synergies-com-597-2005.pdf>; Study finds that “there is no need to introduce new instruments for cross-border information exchange”, *Statewatch News Online*, April 2012, <http://database.statewatch.org/article.asp?aid=31458>

[8] European police to gain access to visa database, *Statewatch News Online*, April 2013, <http://database.statewatch.org/article.asp?aid=32285>

[9] Putting the PNR pieces in place: more EU funding for mass surveillance, *Statewatch News Online*, March 2016, <http://statewatch.org/news/2016/mar/pnr-interconnection-project.html>

[10] Smart borders: “no sufficient evidence” to justify law enforcement access to proposed Entry/Exit System travel database, *Statewatch News Online*, September 2014, <http://database.statewatch.org/article.asp?aid=33953>

and use prints for “electronic identity documents[,] credit cards, loyalty cards or future e-documents.” [11]

The Commission’s Communication puts forth a “long-term approach to interoperability” which would mean setting up “a common repository of data at EU level for different information systems.” However:

“The option of establishing a common repository of data at EU level raises important questions of definition of purpose, necessity, technical feasibility and proportionality of the data processing involved. It would require a complete revision of the legal framework establishing the various information systems and could only be an objective to be achieved in the long-term.”

The “legal, technical and operational questions linked to a common repository of data, including questions of data protection,” are to be addressed first by the new ‘Expert Group on Interoperability and Information Systems’.

The German approach

The Commission’s “long-term vision” on the panoptical future of policing, migration and customs databases and computer networks shares that favoured by the German Federal Ministry of the Interior, which produced a paper on 15 March proposing many of the same ideas. [12]

The interior ministry’s document calls for joining up EU and national databases to provide “integrated identity management for travel, information and security,” due to “the challenges that the EU faces in terms of crises and the influx of refugees.” This will allow “single collection and multiple use” of personal data, the “combination of information that has previously been stored separately,” and “extended political room for action.”

The German paper highlights three sets of problems:

1. Multiple collection of the same information: multiple entries on the same individual in different systems “makes processes more complex, slows them down and increases costs – to the detriment of the authorities collecting data and the travellers concerned”. It fails to meet data minimisation requirements and “increases the risk of errors and insufficient data maintenance” leading to poor data quality. The ministry argues that at border crossings, “manual data collection must be kept to a minimum”: early collection and automation is the future.
2. No information networks: there are too many unlinked databases (both EU and national) and thus “connections” between information are not found “quickly and reliably”.
3. No flexibility: “As a result of the silo-like information architecture, every system discussed here is a complex large-scale IT system” – expensive to set up and operate; and difficult and slow to combine, upgrade or alter.

This makes it “impossible to respond to new challenges in a flexible way”. Furthermore:

[11] INGRESS, http://cordis.europa.eu/project/rcn/110929_en.html

[12] German Federal Ministry of the Interior, ‘Integrated Identity Management for Travel, Migration and Security in Europe’, 15 March 2016, <http://statewatch.org/news/2016/apr/germany-int-min-identity-management.pdf>

“These redundancies are also of operational, legal and political character. The same discussions (e.g. on the registration of biometric characteristics, access requirements for security authorities) take place repeatedly, lead to a distorted political and public perception and often result in unrealistic restrictions that considerably limit the practical use.”

The interior ministry’s solution to these problems is to join together all these databases and networks, “in an integrated system architecture”. This is “complex and will have to be gradually applied to existing and newly introduced systems,” which would seem to call for more of the “same discussions” that the interior ministry bemoans for causing a “distorted political and public perception.” It should be noted that “practical use” may of course be constrained by “unrealistic restrictions” due to the requirements of laws that attempt to restrain state powers and protect individual rights.

Like the Commission, the German proposal suggests a “modular” design: “The core module will contain the basic data on the traveller (i.e. alphanumeric and biometric data)” and will be connected to “specific modules”, “in such a way that they provide the required information”.

Systems that currently involve networked national databases may need to be centralised, which, like the establishment and modification of other IT systems under discussion, sounds complex and costly. The plan is to be “guided by the desire to reduce unnecessary bureaucratic burdens for travellers and security authorities (once-only-principle),” although it seems it will create years of bureaucratic burdens for the officials, civil servants and consultants who will be doing the work.

Standardised systems

The German interior’s ministry’s paper also calls for the use of “state-of-the-art computational approaches (such as the universal messaging format UMF)”.

The Commission last year agreed to give €1.6 million (90% of total funding) to a 30-month project led by Germany aiming to further develop this information standard. A note from Germany to other national delegations in the Council’s information exchange working party (DAPIX) says that:

“UMF3 should be a European exchange standard for law enforcement authorities (LEAs) which is used in case of system adaptations or the development of new systems.”
[13]

17 EU Member States (Bulgaria, Denmark, Germany, Estonia, Greece, Spain, Italy, Latvia, Lithuania, Hungary, Malta, Poland, Finland, Sweden, United Kingdom) and Norway are involved in the project along with the Commission, Europol, eu-LISA and Frontex; Interpol; OLAF [the European Anti-Fraud Office], Eurojust and Switzerland. Europol and various Member States are also undertaking pilot projects to ease access to databases.

The UMF project note also recognises that developing the technical infrastructure required for the swifter exercise of power in the fields of “travel, migration and security” will take time: “The use of the standard is a gradual process which is going to take many years.” This leads to a

[13] German delegation, ‘Universal Message Format (UMF) 3 – Proposal for the 5th IMS action list’, 6882/16, 10 March 2016, <http://statewatch.org/news/2016/apr/eu-council-germany-ims-umf-data-exchange-project-06882-10-03-16.pdf>

need for “an organizational form, the governance model, in order to guarantee the maintenance and further development of the standard.”

Join them up and watch them go

German interior minister Thomas de Maizière has recently proposed that in the name of fighting terrorism, everything “beneath the threshold of changing the treaties” should be done to enhance Europe’s law enforcement and border control databases. [14] This involves doing what the EU and state authorities have been demanding for years: join up everything and provide some sort of “total information awareness” to law enforcement authorities.

Whether the Commission’s whole set of proposals will be taken up with enthusiasm by Member States remains to be seen. Many of the projects mentioned are already underway; others are merely up for “examination”. All the proposals are likely to come under the heading ‘easier said than done’. Calls for the systematic exchange of relevant information between national authorities, and for Member States to make full use of EU agencies such as Europol, frequently go unheeded. Nevertheless, the proposals are far-reaching and require the widest possible debate about the type of society to which they point.

The Commission is apparently keen for discussion to take place:

“Any future initiative would be prepared on the basis of better regulation principles with public consultation and assessment of the impacts, including as concerns fundamental rights and in particular the right to the protection of personal data.”

However, “expert groups” developing “long-term plans” and transnational projects operating on the basis of unspecified “governance models” may not lend themselves to openness, transparency, nor necessarily asking any critical questions. Given that the extension of fingerprinting and facial recognition and the gathering, exchange and merging of ever more personal data is so often considered as a technical matter, the experts may have other issues on their agenda than the political, social and ethical questions at stake.

Statewatch does not have a corporate view, nor does it seek to create one, the views expressed are those of the author. Statewatch is not responsible for the content of external websites and inclusion of a link does not constitute an endorsement.

© Statewatch ISBN . 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 or 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.

[14] EU ‘too clunky to copy German anti-terror model’, *The Local*, 4 April 2016, <http://www.thelocal.de/20160404/germany-against-joint-eu-anti-terror-centre>



Statewatch is a non-profit-making voluntary group founded in 1991. It is comprised of lawyers, academics, journalists, researchers and community activists. Its European network of contributors is drawn from 18 countries. Statewatch encourages the publication of investigative journalism and critical research in Europe the fields of the state, justice and home affairs, civil liberties, accountability and openness.

One of Statewatch's primary purposes is to provide a service for civil society to encourage informed discussion and debate - through the provision of news, features and analyses backed up by full-text documentation so that people can access for themselves primary sources and come to their own conclusions.

Statewatch is the research and education arm of a UK registered charity and is funded by grant-making trusts and donations from individuals.

Web: www.statewatch.org | Email: office@statewatch.org | Phone: +44 (0) 207 697 4266

Post: 356 Holloway Road, London, N7 6PA

Charity number: 1154784 | Company number: 08480724
Registered office: 2-6 Cannon Street, London, EC4M 6YH