Briefing

The interoperability of Justice and Home Affairs databases

Tony Bunyan
(March 2018)

1. Summary of main points

---

a) The Commission’s proposal for interoperable centralised EU databases is justified on the threat posed to internal security by migration and terrorism. This conflation of threats based on fear of the “other” is a classic case of state racism.

b) Building on the above the message is that as the plans only affect 218 million non-EU citizens, so there is no reason for EU citizens to be concerned as it will not affect them. The

assumption that EU citizens are not concerned with the rights and freedoms of non-EU citizens is insulting.

c) Furthermore, the above assertion is untrue. The present plans would mainly affect non-EU citizens but once the centralised EU database is set up it will be extended to include Prüm (vehicle registration, DNA and fingerprint data), ECRIS (criminal records) and the EU Passenger Name Record system (PNR, which will cover internal flights as well as those in and out of the EU) – affecting millions and millions of EU citizens. It is yet another step in EU state-building (See "**The Shape of Things to Come** ", Chapter 6 & 9).

d) The plan is to include all existing, planned and future Justice and Home Affairs (JHA) databases to be run by eu-Lisa.

e) The European Data Protection Supervisor and the Meijers Committee of legal experts are not impressed by the official view that the harmonisation of access across all Justice and Home Affairs database does not present a problem in terms of fundamental rights.

f) The notion that these plans are simply bringing together existing data and biometrics, and so there is nothing to be afraid of is untrue. If there has been one clear lesson since 11 September 2001 it is that function creep is the name of the game.

From the late 1970s onwards each new stage of the technological revolution has been justified on the grounds that there is nothing new, it is just making life easier for law enforcement and border control agencies to get access to the information they need to do their job more efficiently. Whereas the reality is that at each stage databases become ever more intrusive as security demands cumulatively diminish freedoms and rights

2. The plans for the interoperability of JHA databases

The four components in the creation of a centralised EU database are described as:

- A **European search portal (ESP) -** this tool will enable authorised users (for instance an authorised police officer) to carry out a single search and receive results from all the systems they are authorised to access, rather than searching each system individually.
- A **shared biometric matching service (BMS) -** this will allow users to search and cross-match biometric data (currently primarily fingerprints and facial images) stored in the systems that they are authorised to access.
- A **common identity repository CIR)**, which **would contain biographical and biometric identity data of third-country nationals** available in several EU information systems.
- A **multiple identity detector (MID)** - this will verify whether the biographical data that is being searched exists in multiple systems, helping to detect multiple identities. It has the dual purpose of ensuring the **correct identification of *bona fide* persons** and combating identity fraud.

The description of the role of the CIR in the Commission press release hides its crucial role. The Impact Assessment describes its significance as follows:

> *"The **common identity repository (CIR)** would be the **shared component for storing biographical and biometric identity data** of third-country nationals recorded in Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system."* (COM 474-17)

In the first stage the new EU interoperable database will include: the Schengen Information System (SIS), Eurodac (fingerprints of asylum-seekers and, under new proposals, third country nationals who have entered "irregularly") and the Visa Information System (VIS, personal data and fingerprints of short stay visas) plus three new systems currently being negotiated and/or developed: the Entry-Exit System (EES), European Travel Information and Authorisation System (ETIAS, for visa-free arrivals) and the European Criminal Records Information System for third-country nationals (ECRIS-TCN). The new interoperability databases will also be linked to Europol data and Interpol's Stolen and Lost Travel Documents (SLTD) database.

3. The rationale has racist undertones

On 17 December 2017 the Commission presented proposals (**COM 794-17** pdf) which they said will only affect third country nationals entering or living in the EU and not EU citizens:

> *"In the past three years, the EU has **experienced an increase in irregular border crossings into the EU, and an evolving and ongoing threat to internal security as demonstrated by a series of terrorist attacks.** EU citizens expect external border controls on persons, and checks within the Schengen area, to be effective, **to enable effective management of migration and to contribute to internal security.** These challenges have brought into sharper focus the urgent need to join up and strengthen in a comprehensive manner the EU's information tools for border management, migration and security."* [emphasis added throughout]

The Commission **press release** (pdf) adds:

*"In the context of recent **security and migratory challenges, the proposal will ensure greater safety of EU citizens by facilitating the management of the EU's external borders and increasing internal security."***

There are repeated references to migration, internal security and terrorism in the documentation. The European Data Protection Supervisor commented:

> *"**We are concerned that repeatedly referring to migration, internal security and fight against terrorism almost interchangeably brings the risk of blurring the boundaries between migration management and fight against terrorism."***

And the Meijers Committee, a group of legal experts, said:

> ***"This justification basically means that third country nationals should be subject to additional security checks - even if there is no connection to any illegal behaviour - in order to make EU citizens feel more secure.***

4. The centralised database only concerns non-EU citizens

First, the strong implication is that EU citizens need not be concerned with the rights and privacy of non-EU nationals, no responsibility for the "other".

Second, it is clear that while this first phase of interoperability would only affect third country nationals through ECRIS-TCN, the Entry-Exit System, new databases will be added in the future which will involve millions of EU citizens.

Much emphasis is made of the claim that the centralised database will not carry any new information but **the access rights of agencies are being changed to give law enforcement agencies access to all personal data and biometrics held in asylum and immigration databases.** And the Agencies themselves are framing their demands. For example, see the Council Presidency version of: **Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: Update following Council Conclusions on interoperability** (LIMITE doc no: 12223-ADD-1-17, pdf), which contains the demand that:

> *"**Where necessary, change national practice** to ensure that **both law enforcement authorities and security services can insert alerts in the SIS directly without interference of judicial authorities."***

This proposal would clearly limit oversight of which alerts are inserted into the system, offering far greater leeway for misbehaviour, malpractice or simple mistakes.

Another example are Frontex demands for increased access to other databases: **Non-paper by Frontex** (LIMITE doc no: 15174-17, pdf): Frontex says it has less access to data than national authorities. Thus it needs greater access to check third country nationals at external borders with "hotspot" style roles of screening, registration, debriefing and fingerprinting and its role in "returns".

5. Existing and future databases

The Council, Commission and the Security Commissioner expressly foresee JHA interoperability extending to Prüm, ECRIS, API (Advance Passenger Information) and EU-PNR and future databases.

The Commission says in document **COM 793(2017)** (pdf):

> *In addition to these primary operational objectives, this proposal will also contribute to: facilitating the technical and operational **implementation by Member States of existing and future new information systems."***

However, this will come later:

> *"National information systems and decentralised EU information systems are outside the scope of this initiative. **Provided that the necessity will be demonstrated, decentralised systems such as those operated under the Prüm framework, the Passenger Name Record (PNR) Directive and the Advance Passenger Information Directive may at a later stage be linked up to one or more of the components proposed under this initiative."***

Document **COM 794(2017)** (pdf) adds that:

> *"The **shared biometric matching service (shared BMS)** is necessary for the functioning of the ESP [European Search portal], the common identity repository and the multiple-identity detector and facilitates the use and maintenance of the **existing and future relevant EU information systems**."*

The current and future role of eu-LISA is emphasised:

> *"**Implementation plans and monitoring, evaluation and reporting arrangements***
>
> *eu-LISA is responsible for the operational management of large-scale IT systems in the area of freedom, security and justice. As such, it is already entrusted with the operation and technical and operational improvements of **existing systems, and the development of the future systems already envisaged.***"

The Commission had previously convened a High Level Expert Group on Information Systems and Interoperability, which **issued its final reported on 11 May 2017** (pdf). On the very same day, the Council Presidency circulated its response in a **discussion paper on interoperability in the light of the recommendations by the High-Level Expert Group on Information Systems and Interoperability** (LIMITE doc no. 8797/17, pdf), which made clear that it supported the inclusion of all existing and future JHA databases and not just the initial six proposed.

The Council then formalised its position in: **Draft Council Conclusions on the way forward to improve information exchange and ensure the interoperability of EU information systems** (LIMITE document no. 9448/17, pdf)

> *"RECALLING that the Roadmap to enhance information exchange and information management **including interoperability solutions in the Justice and Home Affairs area** (…)*
>
> *CALLS ON Member States, as regards **existing EU information systems**, to fully implement and apply the legislation on the Schengen Information System (SIS), the Visa Information System (VIS), the European Dactyloscopy (Eurodac) **and Prüm Decisions**, and to use these information systems and feed databases covered by those instruments in order to fully exploit their potential"*

The 12th report of the **Security Commissioner** (December 2017, pdf) also refers to the future inclusion of Prüm (providing access to millions of personal records on vehicle ownership in the EU, DNA and fingerprints), ECRIS (access to all national criminal records) and the forthcoming EU-PNR systems (which covers all flights leaving, entering or travelling within the EU).

The Commission's **Impact Assessment** (SWD 473(2017), art II, pdf) emphasises the role of the SIS:

> *"SIS is the largest and most widely used information exchange platform on immigration and law enforcement. It is a centralised system used by 25 EU Member States and four Schengen associated countries, currently **containing 63 million alerts**. These are entered and consulted by competent authorities, such **as police, border control and immigration**. It contains records on third-country nationals prohibited to enter or stay in the Schengen area as well as on EU and third-country nationals who are wanted or missing (including children) and on wanted objects (firearms, vehicles, identity documents, industrial equipment, etc.). **The distinctive feature of SIS in comparison with other information sharing instruments is that its information is complemented by an instruction for concrete action to be taken by officers on the ground, such as arrest or seizure.***

*SIS checks are mandatory for the processing of short-stay visas, for border checks for third-country nationals and, **on a non-systematic basis, for EU citizens and other persons enjoying the right of free movement.**"*

On the Common Identity Repository, the IA noted:

*"**Detailed analysis of the common identity repository***

*The common identity repository (CIR) is not an additional database but **a new IT architecture bringing together existing biographical identity data of third-country nationals (TCNs), such as name, date of birth, travel documents**, that would otherwise have been stored in the various central systems. It is comparable to a shared biometric matching service but handling a subset of biographical data instead of biometric data.*

The CIR enables personal data to be linked to biometrics:

*"The **common identity repository (CIR)** would be the **shared component for storing biographical and biometric identity data** of third-country nationals recorded in Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system."* (COM 474-17)

And:

*"The numbers of biographical data sets that are or will be stored in the respective central EU systems vary substantially, but are **overall in the order of hundreds of millions**."*

In Part I of the Commission's **Impact Assessment** (pdf) it is stated that:

"The total number of people covered by this initiative is estimated to be close to 218 million

- Around 200 million third-country nationals visiting the Schengen area for a short-stay, either as a visa-exempt traveller or with a visa;

- Some 10 million third-country nationals for whom a conviction record in an EU Member State exists;

- Around 7 million asylum seekers and irregular migrants;

- Around 1 million persons for whom an alert is issued in SIS."

Present proposals are setting up the mechanisms for centralised interoperable systems which will serve as a template for and help to facilitate other existing or new databases.

6. European Data Protection Supervisor: "Reflection paper" on the interoperability of JHA databases poses fundamental questions

"Technology should always come in support of policies and user needs, not the other way around. What is technically feasible might not necessarily be legally justifiable or ethically desirable." – European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) published a **"Reflection Paper on the interoperability of information systems in the area of Freedom, Security and Justice"** (17 November 2017, pdf) which poses fundamental questions for the Commission

(responsible for drafting the new measures), the co-legislators (the Council of the EU and the European Parliament), and for society at large. These are quoted at length, under the headings from the paper, below (emphasis added throughout).

b) The concept of interoperability

> *"Interoperability is commonly referred to as the ability of different information systems to communicate, exchange data and use the information that has been exchanged.* ***Although interoperability is often considered as a merely technical concept, we consider that in the present context it cannot be disconnected from the questions whether the data exchange is necessary, politically desirable or legally possible. In other words, although interoperability of the information systems will ultimately be implemented through technical means, it must be subject to political debate on its purposes and future scope.***
>
> *We observe that making exchange of data technically feasible becomes, in many cases, a powerful drive for exchange these data.* ***One can safely assume that technical means will be used, once they are made available; in other words, the risk is that in such case the means justify the end. To allow a proper debate about the risks and advantages of interoperability, it is fundamental to give it an unambiguous and clear meaning.***
>
> *(...) while we note that the Commission might have envisaged interoperability as a tool to only facilitate the use of systems,* ***we understand that the Commission now may aim to extend it to new possibilities of exchanging or cross-matching data.*** *For instance, the inception impact assessment refers to the* ***use of a shared biometric matching service ('the BMS') to enable matching of biometric data held across the various systems. Similarly, a 'common identity repository' would bring together alphanumeric data (such as names and dates of birth) that have been stored in the various systems for border management and security. The combined use of the shared BMS and the common identity repository would enable single identification using alphanumeric and/or biometric data to detect multiple identities. Interoperability thus implies new data processing that are not covered by existing legal bases and their impact on the fundamental rights to privacy and data protection needs to be carefully assessed."***

c) Interoperability from a data protection perspective

> *"We encourage the Commission to* ***clearly describe the specific purposes of the envisaged data processing. Objectives such as "ensuring fast and seamless access to databases" might be a useful means to an end in policy terms.*** *However, they are not specific enough for the purposes of data protection law since they are not linked to specific processing of defined categories of personal data.* ***Consequently, they may not allow individuals to understand which of their personal data are processed for what precise purposes, or to understand the consequences of such processing.***

*(...) we recommend that the forthcoming legislative proposal clearly set out the precise purposes of the various data processing envisaged (...)**"***

"only a clear description of the identified problems in view of the objectives pursued will allow the EU legislator to determine the most appropriate legal and technical solutions, in compliance with data protection law. ***Technology should always come in support of policies and user needs, not the other way around. What is technically feasible might not necessarily be legally justifiable or ethically desirable.****"*

d) Purpose limitation with regard to migration, asylum, police and judicial cooperation

*"**There is an increasing trend in EU policy-making to associate migration management and security purposes.** We see this trend in the context of granting access to existing systems for law enforcement purposes, building a new information system, or extending the competences of an existing body.* ***We are concerned that repeatedly referring to migration, internal security and fight against terrorism almost interchangeably brings the risk of blurring the boundaries between migration management and fight against terrorism."***

e) New uses of data

*"In addition, the information systems that would feed th**e common identity repository had been built for purposes other than combating identity fraud which would constitute a new purpose of data processing.** In this context, **we see a risk of "function creep" (i.e. a widening of the use of a system or a database beyond the purpose(s) for which it was originally intended)**. As with any initiative that would potentially allow for further uses of data or systems beyond what was originally foreseen by law, we would advise a cautious approach. **The argument that, since the data is already collected, they can just as well be used for other purposes cannot be uncritically accepted, since such new processing might have a bigger impact on individuals**."*

f) New security challenges

*"We wish to draw attention on the fact that interoperability - as conceived so far by the Commission - would i**ntroduce a fundamental change in the current architecture of large-scale IT systems: a shift from a closed environment to a shared environment with connectivity between the various systems**. **This would bring about new security risks.** To take the case of the European search portal as an example, such **risks would arise for instance from the fact that <u>an attacker would have to compromise only one single point of access</u> (instead of multiple point of access, i.e. one for each information systems) to get access to several large-scale information systems."***

How many terminals and how many officials have or will have access to all the existing and planned databases and does this present a potential security threat?

In 2003 a Council Presidency: **Report of the ad hoc group for the study of the 3rd pillar information systems** (LIMITE doc no: 8857-03, pdf) stated on page 11 that the:

> *"number of terminals through which the N.SISes [the national Schengen Information System implementations] can be consulted (approx. !!!): 125 000 (cf. document 6739/02 EU CONFIDENTIAL)"* [exclamation marks in original!]

Meanwhile the number of authorities with access has increased significantly as well. in 2013 the list of national "competent authorities which are authorised to search directly the data" in the SIS ran to **116 pages in the EU's Official Journal**. By 2017, that list was **165 pages long**.

7. Interoperability of EU databases – the Meijers Committee's response

The Meijers committee have prepared: **Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, COM (2017) 794** (pdf): Their comments include:

Unintended consequences?

> *"According to the explanatory memorandum,* ***access 'to data is reserved exclusively for duly authorised staff of the Member State authorities or EU bodies that are competent for the specific purposes of each information system and limited to the extent that the data are required for the performance of tasks in accordance with these purposes.'*** [emphasis added throughout]
>
> ***The proposal as such does not alter the specific purposes of the EU databases involved. However, on the basis of the proposal, every designated authority of Member States will be able, via the European Search Portal, to learn about the fact that information on a third-country national is stored in one of the EU databases. In other words, the access of authorities to the European Search Portal is not restricted to their specific competence or task, whereas this specific competence or task currently limits their access to the specific EU databases.*** *Therefore,* ***information retrieved via the European Search Portal will establish that somebody is included in, for example, Eurodac or in SIS II. This implies a widening of the purpose of these databases: even if access to the personal file in this database is not allowed because lack of authorisation, the authority will have gained knowledge of the existence of the file.***
>
> *Moreover,* ***the mere knowledge that a person's data are included in a particular database gives an authority a view of that person's actions, which can in itself be an interference*** *with the right to data protection laid down in Article 8 of the Charter (and with Article 7 of the Charter on the right to privacy). This requires that the proportionality of this access should be assessed."*

Targeting third country nationals

> *"A specific issue in this context relates to the fact that the proposal concerns the interoperability of* ***systems which do not only have different purposes, but also***

include different categories of data subjects. The systems include data of individuals because they are linked to criminal behaviour or illegal border crossing, as well as bona fide persons (included in Eurodac and VIS). It should be explained interoperability will not lead to the mixing up of these categories."

Casting a very wide net?

*"Specifically, t**he explanatory memorandum emphasizes this differentiated treatment between EU citizens and third-country nationals in view of the goal of preserving security in the EU**: 'Whilst not directly affecting EU nationals (the proposed measures are primarily focused on third-country nationals whose data is recorded in an EU centralised information system), **the proposals are expected to generate increased public trust by ensuring that their design and use increases the security of EU citizens. This justification basically means that third country nationals should be subject to additional security checks - even if there is no connection to any illegal behaviour - in order to make EU citizens feel more secure.***

*Furthermore, the **explicit objective of the proposal of facilitating identity checks of third country nationals by police organisation within the EU territory, to see whether information on this person is stored in one or more of the EU databases, will enhance the possibility of third-country nationals (or those considered to be third-country nationals) being stopped for identity checks."***

8. Regulatory Scrutiny Board Opinion: Interoperability

The Regulatory Scrutiny Board is "an independent body of the Commission that offers advice to the College," which provides "a central quality control and support function for Commission impact assessment and evaluation work." Its **Opinion on the interoperability proposals** (SEC(2017) 554 final, pdf) noted a number of shortcomings.

a) Main considerations

*"The Board acknowledges that the impact assessment relies on considerable and detailed technical work. However, the **report still contains significant shortcomings that need to be addressed.** As a result, the Board **expresses reservations and gives a positive opinion only on the understanding that the report shall be further adjusted** in order to integrate the Board's recommendations on the following key aspects.*

*(1) The **report does not sufficiently explain how far the additional measures under its preferred option extend end-users' existing data access rights in EU information systems.** It does not sufficiently explain and illustrate safeguards for data protection and fundamental rights."*

b) Access rights and safeguards for fundamental rights

*"The report should clearly establish **how far the proposed measures would extend existing access rights** for the end-users to EU information systems. **This is particularly relevant for the checks within the territory,** hit-flagging and the Multiple Identify Detector, which are elements of the preferred option.*

*Where options extend access rights, the report should better explain the safeguards it proposes to **manage risks related to data protection and respect for***

fundamental rights, including the right to good administration, the presumption of innocence and the right to defence. *The report should explicitly assess risks of more false positive errors, and discuss any related negative consequences, in particular in terms of freedom and justice. The report should present these risks when it presents expected enhanced security and practical benefits of more efficient IT-systems.*

While this initiative most directly affects non-EU citizens, ***the analysis should also describe any potential (unintended) impacts on EU citizens****. This might include practical examples or a worst-case scenario."*

c) Options and impacts

"The description of the options should clarify how the European Search Portal would integrate data from the Europol and Interpol systems. For ***the Interpol databases which are also fed by third countries****, it should explain how it would ensure respect of fundamental rights."*

9. European Parliament briefing

A **briefing** ("initial appraisal of a European Commission impact assessment", pdf) prepared by the European Parliamentary Research Service followed in the footsteps of the Regulatory Scrutiny Board and made clear a number of issues with the Commission's impact assessment. One issue highlighted was the speed at which it was undertaken:

"The Commission's Regulatory Scrutiny Board (RSB) issued an opinion marked 'positive with reservations' on 8 December 2017. The fact that the IA was published on 12 December 2017 might be indicative of the rush in which it was prepared, but also begs the question as to how the substantial comments of the RSB could possibly have been addressed in the final IA report ***within three working days****. The RSB identified 'significant shortcomings'".*

The conclusions of the parliament briefing stated:

*"The Commission made an effort to build its case for this initiative, however****, the IA displays several weaknesses.*** *The IA would have benefited from clearer problem definition, including indications or evidence regarding the scale of the problems. The range of options is rather limited. The Commission organised a number of stakeholder activities* ***and a public consultation, to which feedback was very limited.*** *The IA is underpinned by the work of the high-level expert group, and also* ***by three supporting studies that are not publicly available at the time of writing****.* ***The fact that the IA was published three working days after the issuance of the RSB opinion raises the question of how the substantial comments of the RSB could have possibly been addressed in the final IA.****"*

10. The argument that there is nothing to worry about as there is nothing new in this proposal ignores lessons from history

There is a view that all the present proposals do is simply to make the systems more efficient and accessible and that there is no new information being created.

A quote from Senator Frank Church who headed a seminal inquiry into the surveillance of the peace movement in the USA (the "Church Committee report", 1975) seems pertinent:

> *"If a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of government to know. Such is the capacity of technology".*

And that was more than 30 years ago.

In the UK it was reported in 1965 that the Special Branch had 2 million people on its card files indexes (Observer, 31 January 1965), with numerous other state agencies maintaining vast numbers of paper records on individuals. When state agencies started computerisation in the late 1970s it was argued that they were merely processing the same information and making things more efficient. But of course this was not the main result of the widespread introduction of computers. Individual files could be further processed to add pictures, fingerprints, videos, contacts, metadata, shared and so on, and information could be combined, processed and used in ways that would have been unthinkable in the age of paper.

In the UK **Crimint** is a database run by the Metropolitan Police Service of Greater London which stores information on criminals, suspected criminals and protesters. It was created in 1994. As of 2005 it contained seven million information reports and 250,000 intelligence records that were available to both police officers and back office staff. As the ***Guardian*** reported:

> *"People are able to request their information from the database under data protection laws.* ***Requests have shown that the database holds large amounts of information on protesters who have not committed any crimes which is to be expected as the database is an intelligence database, not a crime recording system****.*
>
> *Photographs, names and video footage of people attending protests are routinely obtained by surveillance units and stored on an "intelligence system". The - Metropolitan police, which has pioneered surveillance at demonstrations and advises other forces on the tactic, stores details of protesters on Crimint, the general database used daily by all police staff to catalogue criminal intelligence. It lists campaigners by name, allowing police to search which demonstrations or political meetings individuals have attended."*

This is simply an illustration of the power of the application of technology which has shown itself to be continuously adaptable. The EU's proposals for interoperability are more than a simple technical affair and lay the groundwork for ongoing and infinite expansion.

Serious concerns were expressed by the NGO **Privacy International** (pdf) in their submission to the consultation process:

> *"We are concerned that systems proposed which entail a central registry of sensitive personal data such as biometric data raise substantial issues in the context of* ***the history of identification systems throughout the world, which provides evidence of 'function creep'.****"*

And:

> *"Technological systems must support and enhance privacy, not undermine it. If the European Union seeks to implement interoperability in its databases, they must not*

undermine the security of individuals' data. If the information is not properly protected there is the ***potential of unauthorised access to troves of information by third parties, including criminals and agents of authoritarian regimes from which individuals have sought asylum in the EU****."*

Professor Deirdre Curtin, of the European University Institute, observes that some commentators believe the nexus of internal security agencies and law enforcement agencies poses a special problem as they see individuals as objects of surveillance rather than citizens::

> *"The area of security and law enforcement is where information gathering, mining and interoperable sharing is very largely invisible but at the same time subject to accelerated and intensified cooperation. It makes use of vast networks of "data cops" to do its "efficient" work. The problem is, how do we make the invisible transparent? And how do we make informal, unseen and multijurisdictional arrangements accountable?" ('Security of the interstice and interoperable data sharing: A first cut', in Constitutionalising the Security Union, CEPS, 2017).*

11. Key documents

On 12 December the European Commission put forward proposals to link all Justice and Home Affairs databases into one centralised system.

Press release

Security Union: Commission closes information gaps to better protect EU citizens (press release, pdf) covering: *"security, border and migration management."*

The two proposed Regulations

Regulation on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 (COM 793(2017), pdf)

Regulation on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) (COM 794(2017), pdf)

Impact Assessments

Staff Working Document - Part 1 (COM SWD, 473, pdf) and **Staff Working Document - Part 2** (COM SWD, 473, pdf)

12. Background

Interoperability of EU databases - The Meijers Committee (Statewatch News, 17.2.18)

EDPS **"Reflection paper" on the interoperability of JHA databases poses fundamental questions** (Statewatch News, 2.12.17)

"Interoperability": Plans to link all Justice & Home Affairs databases into one centralised system - repeated references to migration, internal security and terrorism (Statewatch News, 17.12.17)

JHA Roadmap on interoperability: Agencies get moving (Statewatch News, 26.10.17)

Council: EU JHA agencies want access to all fingerprints, palm prints and facial images held under interoperability plans (Statewatch News 24.9.17)

Interoperability and EU databases: Big Brother takes shape (Statewatch News, 29.6.17)

Commission wants a quick march to interoperable, centralised EU databases by 2020 (Statewatch News 17.5.17)

EU wastes no time welcoming prospect of Big Brother databases (Statewatch News 15.5.17)

Plans to boost information-gathering and exchange by law enforcement authorities and agencies - implementation report (Statewatch News, 15.5.17)

Council, Europol and "expert group" press on with plans to boost "information exchange and information management" (Statewatch News, September 2016)

The Shape of Things to Come: Chapter 6 (2009)

The "principle of availability": the free market in access to data/intelligence will rely on "self-regulation" by the law enforcement agencies and make accountability almost meaningless (December 2006).