Analysis

The “point of no return”

Interoperability morphs into the creation of a Big Brother centralised EU state database including all existing and future Justice and Home Affairs databases

Tony Bunyan

May 2018

1. Introduction

This Analysis looks at key critiques of EU plans to create a pervasive EU state database covering existing and future Justice and Home Affairs databases. [1]

What started out as creating "interconnectivity" between EU JHA databases was quickly rejected by the High Level Group of Experts in favour of "interoperability" which in turns has morphed at the hands of the Council and the Commission into the creation of a centralised EU state database covering all JHA databases.

In fast-moving scenarios the institutions' argument that only databases concerning non-EU citizens would be affected was undermined by the stated aim to covers all JHA databases (eg: EU PNR, treating all travellers as potential suspects and the ECRIS – European Criminal Records Information System) involving millions of EU citizens.

In an innocuous "policy debate" Council document the Council Presidency asked Member States:

> *"**Do you consider that any additional elements should be considered in the current legislative proposals on interoperability, such as should storing biometric data from national databases**, Europol and Interpol in the **shared Biometric Matching Service?"2*** [emphasis added throughout]

This would cover millions of DNA samples and fingerprints held in the national- based Prüm system which is already on the list of existing databases to be incorporated after the first stage.

Then on 17 April 2018 came a proposal from the Commission for a Regulation for national ID cards to include mandatory biometrics (fingerprints and facial images) covering over 370 million EU citizens. [3]

Will this lead to another case of "function creep"?

---

[1] In 1991 I wrote an article in a special issue of *Race & Class: Europe variations on a theme of racism* (volume 22 no 3, January-March 1991, pp.19-31) entitled 'Towards an authoritarian European state'. Nothing that has happened since has changed my mind. In March 1991 Statewatch was launched with the primary objective of monitoring and analysing the emerging EU state. This is a process which is still underway through state building. As Professor Bob Jessop observes in his book: "The State, past present and future" (2016) the European Union is a "state in the process of formation" (p.137).

[2] Council document no. 6396-18 (pdf), 26 February 2018

[3] Proposal for a Regulation on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (COM(2018) 212 final, pdf) and Impact assessment and see SWD (2018) 110 final (pdf): *"Many of the EU's security measures rely upon secure travel and identity documents – such as the systematic checks established by the Schengen Border Code13 in the Schengen Information System. Enhancing the exchange of information through the interoperability of EU information systems for security, borders and migration management as recently proposed by the Commission, will also depend on enhanced document security, including for conducting identity checks by competent authorities within the territory of EU Member States."* (p.3)

2. Background

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

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.

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."* [4]

This Analysis looks at the opinions and contributions from the European Data Protection Supervisor, the Article 29 Working Party on data protection and the European Parliament. [5]

3. The European Data Protection Supervisor (EDPS) [6]

> *"**Interoperability is not primarily a technical choice, it is in particular a political choice to be made.** Against the backdrop of the clear trend to mix distinct EU law and policy objectives (i.e. border checks, asylum and immigration, police cooperation and now also judicial cooperation in criminal matters) as well as granting law enforcement routine access to non-law enforcement databases, **the decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure** and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would **as such mark a 'point of no return'.** For these reasons, the EDPS calls for a wider debate on the future of the EU information exchange, their governance and the ways to safeguard fundamental rights in this context."*

[4] Executive summary of the impact assessment, SWD(2017) 474 final, 12 December 2017, https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-474-F1-EN-MAIN-PART-1.PDF
[5] See also: Fundamental Rights Agency report on interoperability (pdf)
[6] Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems (pdf)

> *"**A central database - in contrast to decentralised databases - implicitly increases the risk of abuse and more easily rouses desires to use the system beyond the purposes for which it was originally intended.** It is therefore necessary to closely scrutinise the Proposals, paying particular attention to the existence of all necessary safeguards."*

For this reason, the scale and nature of the data stored on a centralised database – the CIR (Central Identity Repository) – could "seriously harm a potentially large number of individuals."

The EDPS says in recent years there has been an increasing trend to equate the real or imagined threats posed terrorism and migration and demands for law enforcement agencies (LEAs) to have access to migration and asylum databases:

> *"By creating interoperability between migration, police cooperation but also judicial cooperation tools, the Proposals are part of this trend. As already stressed in his reflection paper, **the EDPS is 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 crime and terrorism. It may even contribute to creating assimilation between terrorists, criminals and foreigners.**"*

Furthermore, giving LEAs access to non-law enforcement systems is:

> "*far from insignificant from a fundamental rights perspective. **Routine access would indeed represent a serious violation of the principle of purpose limitation.** The EDPS therefore calls for the maintenance of genuine safeguards to preserve fundamental rights of third country nationals."*

Moreover:

> *"The CIR would facilitate the **identification of persons including on the territory of Member States** and also help streamlining the access by law enforcement authorities to non-law information systems. **The CIR would store biographical and biometric data recorded in the VIS, the ECRIS-TCN, the EES, the Eurodac system and the ETIAS."***

The EDPS recognises the need for the more efficient use of large scale data systems on migration and terrorism but "the need for better exploitation of the data should never lead to the violation of the fundamental right to data protection."

The EDPS is of the opinion that the proposals:

> *"**ultimately contribute together to establish a central database of third country nationals, in particular a central biometric register of third country nationals**."*

The Common Identity Register

> *"As a preliminary remark, the EDPS would like to stress that the CIR will store data about **all third country nationals that have crossed or are considering crossing the EU borders (with a few exceptions), i.e. millions of people**. **These data include biometric data which are, by nature, very sensitive. Indeed, unlike other personal data, biometric data are neither given by a third party nor chosen by the individual; they are immanent to the body itself and refer uniquely and permanently to a person.** Besides, **a database is all the more vulnerable, sought-after and subject to multiple uses as it is large, connected to thousands of access points and it stores sensitive data such as biometric data."***

The EDPS expands on this last point about thousands of access points to the planned centralised database:

> *"the **consequences of any data breach affecting the CIR could seriously harm a potentially large number of individuals. If ever it falls into the wrong hands, the CIR could become a dangerous tool against fundamental rights** if it is not surrounded by strict and sufficient legal, technical and organizational safeguards. Special vigilance is therefore essential both as regards the purposes of the CIR as well as its conditions and modalities of use."*

The contentious Article 20

One of the most controversial new uses of the centralised database will be for police and border guards to use the CIR to check biometric identities and hence the biographical details of a person being identity checked by officers. This new power under Article 20 can, and will, clearly not be limited to non-EU citizens as its primary purpose to is vary out checks on people inside the EU – who may become the subject of a check due to their colour – effectively racial profiling.

The EDPS observes:

> *"Article 20 of the Proposals provides that **a Member State police authority may query the CIR with the biometric data of a person taken during an identity check solely for the purpose of identifying this person.** Such access must be provided by national law. **The law shall specify the precise purposes of the identity checks within the framework (as part) of preventing and combating irregular migration and/or contributing to a high level of security.** It shall also designate the police authorities competent and lay down the procedures, conditions and criteria of the checks."*

The justification for this new power offered in the Commission's Impact Assessment is that Member States do not have records for people on short-stay visas.

> *"The EDPS stresses **that "combating irregular migration and ensuring a high level of security" is a very broad description of (otherwise legitimate) purposes.** He notes that Article 20 requires the adoption of a national law that shall further define them. However, he would like to recall that the Court of Justice of the European Union ('CJEU') in its Digital Rights Ireland ruling held that the Directive 2006/24 **failed to 'lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences' by simply referring 'in a general manner to serious crime, as defined by each Member State in its national law.' The Court also considered that the purpose for the access and use of the data was not 'strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto."***

For these reasons the EDPS recommends:

> *"**The EDPS considers that the purposes of combating irregular migration and contributing to a high level of security in the context of Article 20 are too broad and do not fulfil the requirements of being 'strictly restricted' and 'precisely defined' in the Proposals, as required by the Court. He therefore recommends to further define them in the Proposals**. For instance, "irregular migration" could refer to the conditions of entry and stay as set out in Article 6 of Regulation (EU) 2016/399 of the European Parliament and of the Council. As regards security, the EDPS*

recommends to target the criminal offences that could in particular threaten a high level of security; for ***instance by referring to the crimes listed in Article 2(2) of Framework Decision 2002/584/JHA*** *if they are punishable under national law by a custodial sentence or a detention order for a* ***maximum period of at least three years."*** [7]

"*Therefore, the EDPS recommends to amend Article 20 to provide that access to the CIR will be allowed:*

- ***in principle, in the presence of the person and,***

- ***where he or she is unable to cooperate and does not have document establishing his/her identity or,***

- ***refuses to cooperate or,***

- ***where there are justified or well-founded grounds to believe that documents presented are false or that the person is not telling the truth about his/her identity***." [emphasis in original]

LEA access to migration databases

The EDPS says that "facilitating the access by law enforcement authorities to non-law enforcement systems (even to limited information such as a hit/no hit) is far from insignificant from a fundamental rights perspective:

*"One must bear in mind that those systems have been set up and developed in view of the application of specific policies and not as a law enforcement tool****. Routine access would represent a violation of the principle of purpose limitation. It would entail a disproportionate intrusion in the privacy of for instance travellers who agreed to their data being processed in order to obtain a visa, and expect their data to be collected, consulted and transmitted for that purpose.*** *Moreover,* ***removing genuine safeguards introduced to preserve fundamental rights mainly in the interest of speeding up a procedure would not be acceptable. If there is a need to improve the procedure, this should not be done at the expense of safeguards."***

Safeguards against "fishing expeditions"

The EDPS notes that under Article 22 one of the primary conditions to access the systems no longer applies "i.e. the reasonable grounds to consider that consultation will substantially contribute to the prevention, detection or investigation of a terrorist offence or of other serious criminal offences":

"A reasonable ground could for instance be a fake travel document found on a scene of a crime. He considers that ***the requirement to have reasonable grounds is a fundamental pre-requisite of any access by law enforcement authorities to non-law enforcement systems. This is indeed an essential safeguard against possible 'fishing expeditions'****."*

[7] It is interesting to recall that the above Framework Decision defines a serious crime as one that brings at "at least three years" when some EU states seek to lower the threshold to six months. See: UK gov admits Investigatory Powers Act illegal under EU law, *The Register*, 30 November 2017

Transitional period

The easily missed provision on the "transitional period" makes absolutely clear the role of the new EU state CIR centralised database:

> *"The EDPS understands that in accordance with recitals 21, 22 and Article 17(2) of the Proposals, the CIR would store the personal data (biographic and biometric data) of third country nationals from the EES, VIS, Eurodac, ETIAS and ECRIS-TCN. It is also clear that these data would not remain in the aforementioned systems**, as CIR will be "a central architecture that shall replace the central systems".***

4. The Article 29 Working Party [8]

The Article 29 Working Party on data protection (WP) regrets that the Impact assessments accompanying these two proposals fail to give a detailed analysis "to clarify which data protection regime will apply to which operation and no evaluation of the specific security measures needed for these new EU-wide databases is foreseen" and in addition:

> *"no analysis **of less intrusive means to reach the goals** set in these proposals has been provided to justify the choices made (…)*
>
> *the process towards the interoperability of **systems raises fundamental questions regarding the purpose, necessity and proportionality of the data processing involved as well as concerns regarding the principles of purpose limitation,** data minimization, data retention and clear identification of a data controller."*

European Search Portal (ESP)

As regards the ESP the question arises whether the ability to carry out one centralised search of all the underlying databases can pose an additional interference in itself with the rights to privacy and data protection:

> "*As regards the necessity of the European Search Portal, the WP29 is of the view that **the justification advanced concerning the facilitation of the technical and operational implementation by Member States of existing and future new information systems cannot be considered as an acceptable demonstration of the necessity of this tool**."*
>
> *"The European Search Portal is capable of giving an overview of all the information relating to a certain TCN that is available in the connected EU information systems as well as Europol data and Interpol systems and therefore **requires caution in particular in respect of the impact on data subjects' rights deriving from search tools.***
>
> *Even if the Portal does not accumulate the available data from these information systems with data from additional sources, the result is **related to different matters such as travel, migration, international protection, law enforcement and judicial proceedings.** Therefore, although this tool may not be sufficient in itself to establish a more or less detailed profile of the data subject concerned, **it is important to ensure that – in particular when additional functions or additional access rights than***

[8] Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration (pdf)

> ***the existing ones are envisaged - the establishment of a European Search Portal does not lead to an additional interference with the rights to privacy and data protection**."*

Common Identity Repository (CIR)

The WP notes that the Common Identity Repository (CIR) is a "**new database with the biometric and alphanumeric identity data"** extracted from all the underlying systems.

The WP draws attention to a ruling by the Court of European Justice (CJEU) which indicates that the central storage of biometric data – as distinct from local storage – needs "more stringent requirements than their local storage in an ID-document in the possession of the data subject."

The WP reiterates it previously stated view that

> *"there is no discussion of any alternative solutions in the Commission's Impact Assessment**. For example, to issue some kind of EU identity paper including biometric identifiers and to put an obligation on TCN to carry it with them might appear a less intrusive but equally appropriate measure,** for example. So far in the view of the WP29, the necessity of a consolidated database including biometric identifiers has not been established yet and the **mere fact that some databases containing these types of data have already been created and constitute precedents does not demonstrate this necessity.***

The WP previously underlined that "*there is a risk that the setting up of a centralized database containing personal data and in particular biometric data of all (European) citizens could infringe the basic principle of proportionality."*

And:

> "*The ECtHR has itself drawn a clear line in its ruling that **the retention of fingerprints in a central biometric register solely for the reason of preventing future identity theft would, in practice, allow for the storage of information on the entire population, which would be clearly excessive** (without additional specific guarantees, such as the effective right to obtain the deletion of the data for the concerned data subjects.).*" [9]

Biometric Matching Service (BMS)

The Working Party says that:

> *"The **necessity and proportionality are equally questionable here**, since in addition the BMS **will not be restricted to biometric templates on TCN, but also include templates of EU citizens being subject to any kind of alert in the field of police and judicial cooperation in criminal matters."***

Article 20

The WP is particularly concerned about the use of Article 20:

> *"providing for the possibility to access the CIR for the sole purpose of identification of a person, **irrespectively to the existence of access rights to the underlying data bases feeding the CIR, as it would be the case for police authorities in the context of Article 20, would raise serious concerns as regards the purpose***

[9] ECtHR, No. 19522/09, M.K. v. France, 18 April 2013, para. 40, http://hudoc.echr.coe.int/eng?i=001-157565

limitation principle and the proportionality of this provision. Indeed, the mere fact that the setting up of the CIR results in the creation of a centralised data base does not justify that access to this data base for the purpose of identification of a person is justified in itself."

And:

"The WP29 would like to stress ***its major concern as regards the creation of access rights to an EU-wide data base on the sole justification that this data base is available and that such access would be of added value, in this case for police authorities."***

In addition:

"the Working Party would like to underline that querying the CIR for the purpose of identification of a person ***could result in a very large number of accesses given the volume of identity checks led by police authorities."***

Amongst the WP's conclusions are:

"As regards the necessity of ***the European Search Portal (ESP)****, the WP29 is of the view that the justification advanced concerning the facilitation of the technical and operational implementation by Member States of existing and future new information* ***systems cannot be considered as an acceptable demonstration of the necessity of this tool.****"*

"Regarding ***the Common Identity Repository (CIR)****, the WP29 is of the view that the cross-matching of various sources for identification and consolidating them in a new common data base for the purpose of overall identification* ***poses an additional interference with the rights to privacy and data protection****. The WP29 is not convinced of the necessity and proportionality to establish such a mixed-purpose identification database including biometric data. Whether identity fraud is in practice* ***such an essential threat to the internal security of the Union as to justify the central registering of biometric identifiers of all bona fide TCN travellers, migrants and asylum seekers is not yet sufficiently established in terms of proportionality and therefore remain an issue of major concern.****"*

5. European Parliament study [10]

The conclusions of the European Parliament's study focus on the definition of interoperability and Article 20:

"In the Commission's legislative proposals on establishing a framework for interoperability between EU information systems, however, ***the definition appropriated for the concept of interoperability is not explicitly stated and not sufficiently elaborated****, as most prominently highlighted by the EDPS.(…)*

"Commenting on the 2016 Communication on stronger and smarter information systems for borders and security, the EDPS notes that the Commission's work ***focuses on interoperability as a technical concept, without fully considering whether the data exchange is 'necessary, politically desirable or legally possible'****. As such, the EDPS calls for a clear and unambiguous meaning for*

[10] Interoperability of Justice and Home Affairs Information Systems, April 2018, http://www.statewatch.org/news/2018/apr/ep-study-interoperability.pdf

interoperability and suggests that existing assumptions result in a misaligned focus for the proposed general objectives."

The study calls for "much greater clarity":

> *"the **biggest challenge facing the proposals is that, in reality, they do not establish a framework for interoperability, but instead propose technical solutions, some of which are compatible with the concept of interoperability, some of which are not**. And, as mentioned above, the understanding of interoperability appears to be based on the solutions conceived as opposed to the solutions being created based on a clear, transparent and agreed understanding of interoperability. **With this in mind, interoperability needs to be clearly defined, including its outer limits, otherwise it may become a flexible concept and a moving target."***

Article 20 stops and checks

> *"The proposed **identity checks on the territory of the Member States for the purposes of police investigations that do not reach the threshold of serious crimes** has the potential to negatively impact several Fundamental Rights of the EU Charter. The proposal potentially increases the risk of discrimination of third-country nationals on the basis of racial or ethnic origin, infringing on **the right of non-discrimination (Article 20 of the Charter)**. The proposal's intention to extend the use of interoperable systems to permit identity checks on third-country nationals may increase the possibility of stopping third-country nationals for checks, **which can be construed as inherently discriminatory."***

Central Identity Repository

> *"**the establishment of the CIR is the most invasive dimension of interoperability** – as conceived by the Commission – and raises privacy and data protection concerns in numerous respects."*

Biometric Matching Service

> *"The proposals anticipate that such security measures would 'generate increased public trust by ensuring that the… design and use [of interoperable systems] increases the security of EU citizens'. **the sBMS constitutes a new database and therefore does not conform to an appropriate definition of interoperability."***

6. Conclusions

These three critiques confirm the initial conclusions drawn in Statewatch's Briefing produced in March 2018: **The interoperability of Justice and Home Affairs databases** (pdf) and additionally emphasise three key aspects:

a) the notion of "interoperability" has been replaced by the creation of a centralised EU state database incorporating existing and future decentralised national databases.
b) the widespread and discriminatory use of internal police checks under Article 20 would affect non-EU citizens and EU citizens alike.
c) the planned introduction of national biometric ID cards across the EU could cover 370 million EU citizens as things stand and most likely will be added to the central EU state database in the future.

Previous conclusions

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**", chapters 6 and 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 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.

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: (00 44) 203 691 5227

Post: c/o MDR, 88 Fleet Street, London EC4Y 1DH

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