Executive Summary

Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status

statewatch

PICUM
PLATFORM FOR INTERNATIONAL COOPERATION ON UNDOCUMENTED MIGRANTS

Figure 1: New interoperability systems expected to be in place by 2023

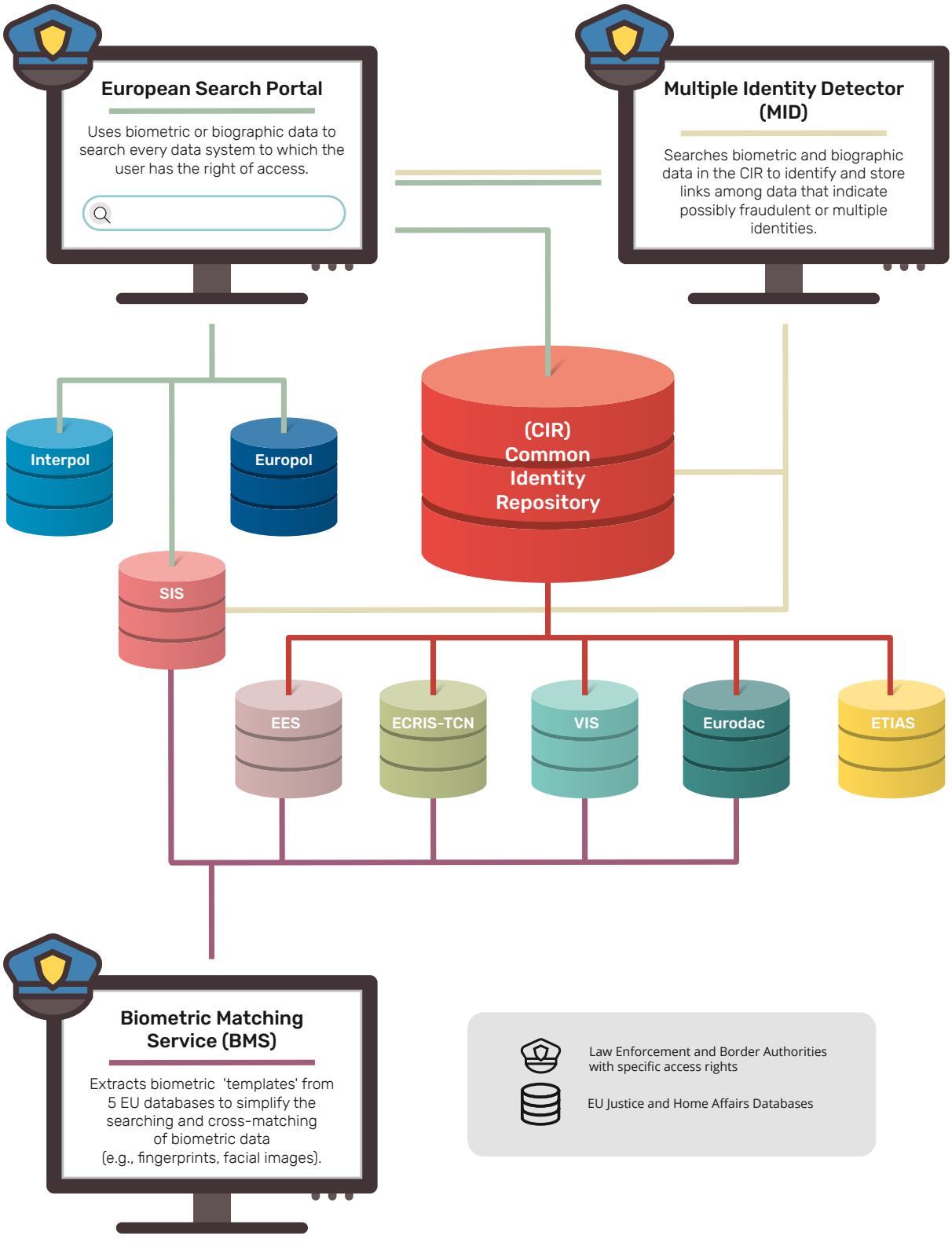
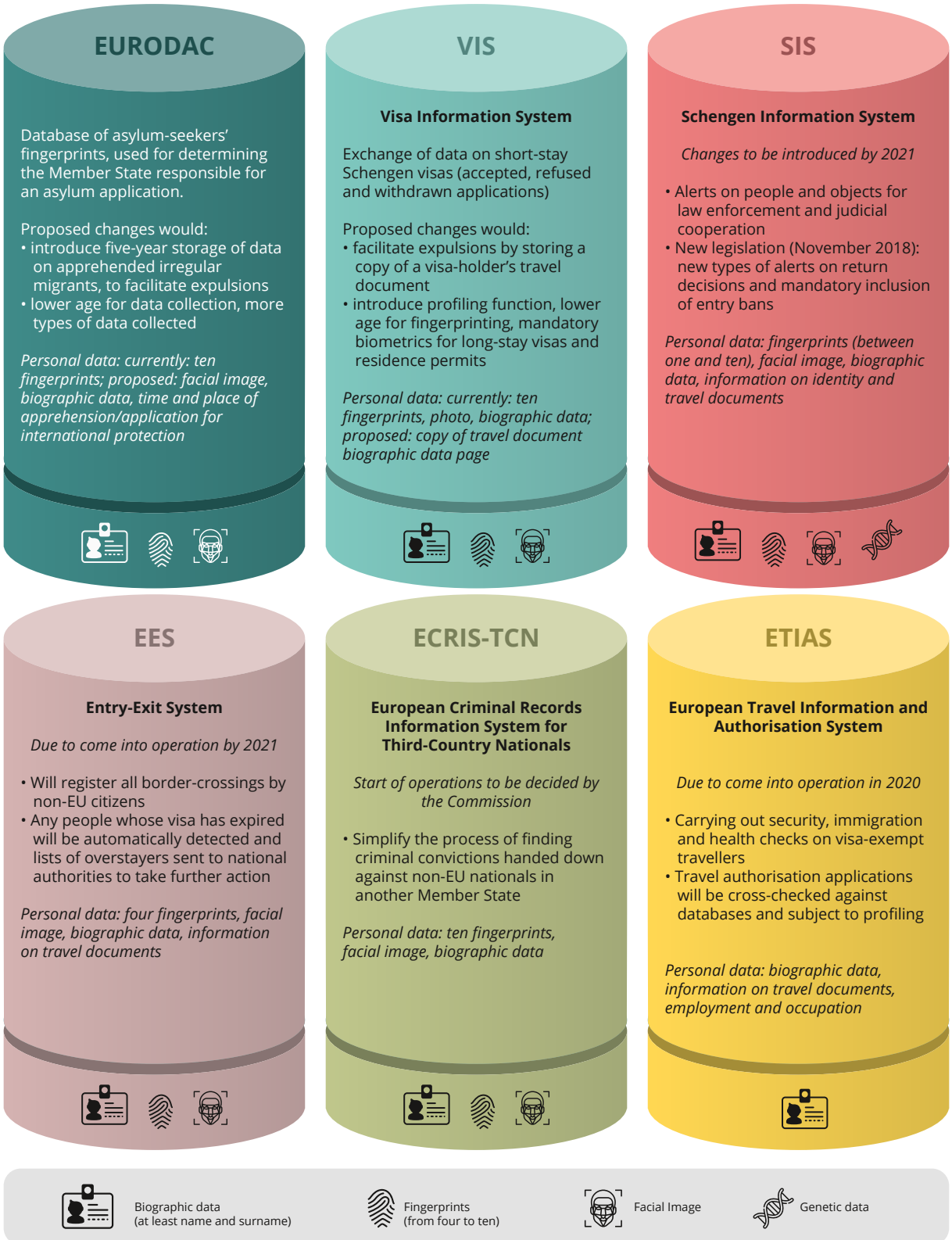


Figure 2: **Existing and forthcoming EU Justice and Home Affairs databases**



Executive Summary

This paper examines the EU's justice and home affairs databases and information systems, the changes that have been introduced by recent legislation seeking to make those systems 'interoperable' and the potential implications of those changes for fundamental rights, in particular in relation to undocumented migrants. Notwithstanding concerns over the necessity and proportionality of the interoperability initiative as a whole, the new rules lack the necessary safeguards to protect people from the arbitrary, unjustified or excessive exercise of state power. With key details left to national government decisions, closely monitoring the implementation of these rules will be crucial to uphold the rights of undocumented migrants and other parts of the population.

Massive data processing to facilitate increased identity checks

One key aim of the interoperability initiative is to facilitate an increase in police identity checks of non-EU nationals, whether documented or undocumented. To this end, a huge new database – the **Common Identity Repository (CIR)** (see Fig. 1), with a capacity of up to 300 million records containing biographic and biometric data – is being constructed, making use of data in a number of existing and forthcoming EU databases.

This paper focuses on four main issues arising from the legislation governing how national authorities should use the CIR for carrying out identity checks:

- while the legislation contains anti-discrimination safeguards, they are extremely weak;
- there is no evidence to suggest that non-EU nationals are more likely than EU nationals to be engaged in activities threatening public security or public policy, calling into question the proportionality of allowing access to the CIR for the broad purpose of "ensuring a high level of security", as it suggests that non-EU nationals *a priori* constitute a security threat;
- the legislation does not precisely circumscribe the specific offences or legal thresholds that could justify access to the database; and
- depending on the way Member States implement EU rules on data protection in the criminal justice and law enforcement sector, the CIR could be used to undermine 'firewalls' between public services and immigration enforcement.

Repurposing data from underlying IT systems

The way the CIR is being constructed also runs counter to a key data protection principle. The data it will contain (at least one biometric identifier and basic biographic details, in essence equivalent to that available in the chip of a biometric passport) is to be extracted from a number of existing and forthcoming systems (**EES**, **ETIAS**, **Eurodac**, **SIS**, **VIS** and **ECRIS-TCN**, see Figure 2). As well as being used to facilitate identity checks and assist in criminal investigations via the CIR, this data will be subject to large-scale, automated cross-checking to try to detect the use of multiple identities by non-EU nationals, through the introduction of a system called the Multiple Identity Detector (MID).

These underlying databases were set up for specific purposes, such as the issuance of short-stay Schengen visas (the VIS) or the registration of crossings of the external Schengen borders (the EES). The use of data for new purposes that were never foreseen in the original legislation – as will be done with the CIR and the MID – undermines the principle of purpose limitation: personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".[1] While the relevant legislation has been amended to graft new purposes onto the existing systems, the necessity and proportionality of doing so is highly questionable.

1 Article 5(1)(b), General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Existing systems reformed for an expanded role in detection and expulsion

Recent and ongoing changes to the legislation governing the EU's databases do not only seek to ensure that the information they hold can be used in the CIR and the MID. Three long-standing databases – the **Schengen Information System**, **Eurodac** and the **Visa Information System** – have recently been or are being reformed. A key aim of the changes is to expand their role in the detection and expulsion of those with no right to remain in the Schengen area.

The changes to Eurodac (for which negotiations are ongoing) will have a particular impact on undocumented migrants. The Eurodac proposal seeks to transform what is currently an asylum database into one for "wider immigration purposes" by introducing the five-year storage of personal data from third-country nationals or stateless persons found irregularly staying in a Member State. The aim is to help identify those who should be subject to expulsion orders and provide "precious elements of evidence for re-documentation and readmission purposes."[2]

Currently, data on this category of persons may be checked against the central Eurodac database (which holds the fingerprints of asylum-seekers and individuals apprehended in connection with irregular border-crossings) but it is not stored. If the changes are approved as proposed, their data would be stored in Eurodac and also added to the CIR, where it would be used to facilitate identity checks aimed at detecting undocumented migrants. Even without these changes, however, the absence of an individual from the CIR may lead to suspicion on the part of the authorities regarding their immigration status.

A fundamental shift in data processing to support immigration and law enforcement

The interoperability initiative will introduce fundamental changes to the structure and operation of the EU's justice and home affairs databases and the processing and use of the personal data they contain. In relation to the 'identity data' of non-EU nationals, the interoperability rules introduce a "single, overarching EU information system" – something that just a decade ago the European Commission argued would "constitute a gross and illegitimate restriction of individuals' right to privacy and data protection."[3]

At the same time, the databases underlying the new 'interoperable' systems are being altered to try to more effectively and efficiently locate and expel those who are irregularly present in the Schengen area, through the processing of more personal data, gathered from a greater number of people, for a broader set of purposes. The potential effects for non-EU nationals, including undocumented migrants, are likely to be significant. Migrants' rights and privacy advocates should pay close attention to the changes being introduced at EU level, the framing of forthcoming national legislation concerning identity checks, the development and implementation of the systems themselves and emerging plans that seek to expand the new 'interoperable' systems to include EU nationals.

2 Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac', COM(2016) 272 final, 4 May 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272

3 European Commission, 'Overview of information management in the area of freedom, security and justice', COM(2010) 385 final, 20 July 2010, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/news/intro/docs/com_2010_385_en.pdf

PICUM

PLATFORM FOR INTERNATIONAL COOPERATION ON
UNDOCUMENTED MIGRANTS

statewatch

This report was written by Chris Jones, Researcher at Statewatch, as a background document for a legal seminar organised on 14-15 November 2019 in Brussels by PICUM, the Centre for European Policy Studies (CEPS) and European Migration Law.

PICUM gratefully acknowledges the support of Emer Connor, PICUM trainee, for her assistance in finalising the report.

The legal seminar and the preparation of this report were made possible through the generous support of:

European Commission

SIGRID RAUSING TRUST

OPEN SOCIETY FOUNDATIONS

ADESSIUM FOUNDATION

OAK FOUNDATION

Epim European Programme for Integration and Migration

This report has received financial support from the European Union Programme for Employment and Social Innovation "EaSI" (2014-2020). For further information please consult: http://ec.europa.eu/social/easi. The information contained in this publication does not necessarily reflect the official position of the European Commission