Building the biometric state: Police powers and discrimination
1. Introduction

2. Biometric identification: a European priority
   - Asylum-seekers: the first target group
   - From asylum-seekers to citizens and residents
   - Onwards to interoperability

3. Funding for biometric technologies
   - Biometrics and security research
   - Advancing state and industrial interests

4. Police technology networks

5. Advanced technology, regressive practices
   - Ethnic profiling by police
   - Interoperability for identity checks

6. Conclusion
1. Introduction
The use by states of biometric technology for identifying individuals has proceeded apace over the last three decades. Initially reserved for use in fixed locations such as police stations, consulates (for example, for visa processing) or detention centres, it was subsequently extended to borders, with fingerprints and facial images now captured and verified at border crossing points in multiple countries around the globe. Some states have also sought to equip police officers and immigration officials with mobile biometric identification devices that make it possible to scan fingerprints or faces in the street to verify an individual’s identity. Under the aegis of the EU’s ‘interoperability’ initiative, which will interconnect a host of different personal data, these efforts at mobile biometric identification are due to expand significantly.

This report examines the development of laws, projects and policies designed to advance the development and deployment of biometric technologies for the purposes of individual identification in the European Union over the last two decades. Following the establishment of separate systems for the collection and storage of biometric data on different categories of foreign nationals – from asylum-seekers to visa-holders to refugees and others – data is now being made ‘interoperable’ through consolidation in a single, overarching database. This will provide the technical foundation for policies aimed at stepping up identity checks, with the primary aims of combating identity fraud and increasing the number of deportations.

This poses significant risks for the rights of citizens and non-citizens alike. In a context of entrenched ethnic profiling by law enforcement officials, the provision of new technological means for carrying out identity checks is likely to exacerbate existing discriminatory practices. This calls for renewed efforts by campaigners, activists, lawyers and researchers to investigate, analyse and challenge both the development and acquisition of new policing technologies, and the laws and policies underpinning their use.

The first section of the report examines the gradual development of an overarching biometric identity system at EU level, starting from the establishment of Eurodac (a database for storing asylum-seekers’ fingerprints) at the turn of the century, to the ongoing construction of the Common Identity Repository (CIR), which will integrate biometric and alphanumeric data from five different large-scale databases. It appears that national authorities have so far made little progress in acquiring the technology needed to conduct identity checks using the CIR, indicating the possibility for interventions to ensure that – at the very least – meaningful equality and data protection impact assessments are carried out prior to its introduction.

The following section examines how public funding from the EU’s research and innovation programmes has contributed to the development of biometric identification technologies, in particular those that have later been incorporated into initiatives such as ‘smart borders’. The EU has awarded some €290 million in public funding to the development of biometric technology since 1998. Over the last 15 years, propelled by the war on terror and the search for technological ‘solutions’ to issues such as crime, terrorism and irregular migration, the majority of this funding has gone towards research projects focusing on public security applications for biometrics. EU agencies such as Europol and Frontex are now being given roles in determining research priorities, with the aim of ensuring that the needs of police and border agencies are taken into account. In response, increased public and democratic scrutiny of the programme is required.

The report subsequently elucidates the secretive networks of policing and technology specialists that have sought to refine the policies and practices needed to put these technologies into use, before going on to examine the context into which those technologies are being deployed: one of long-standing ethnic profiling by law enforcement authorities. The introduction of new technologies into this context, with the explicit aim of easing identity checks, is likely to see an increasing number of unwarranted checks against ethnic minority citizens and non-citizens, given the way in which skin colour is all-too-often treated as a proxy for immigration status.

The report includes a number of case studies that seek to illustrate ways in which states have sought to collect and use biometric data in recent years, and to highlight some of the important challenges from civil society actors in response. There are a growing number of initiatives that seek to make connections between anti-racist campaigns, migrants’ rights organisations and technology specialists. This will prove vital in the years to come as states increasingly seek to use new technologies to enforce divisive and exclusionary laws and policies.

In a world in which biometric identification systems are increasingly-present in technologically-advanced societies, it is no surprise that state authorities also seek to make use of them. The introduction of these schemes is generally justified on the grounds that they aid in regulating international mobility, fighting crime and terrorism, and combating ‘illegal’ immigration. This may, in part, be true – but they also grant the state historically unprecedented powers vis-à-vis the individual. In a context of systemic racism and discrimination and a continued drive by both national governments and EU institutions to identify increasing numbers of foreign nationals in order to deport and/or exclude them from their territory, the attempt to extend and entrench the deployment and use of biometric technologies must be interrogated and challenged, as part of the broader fight against state racism and ethnic profiling, and for racial equality and social justice.
2. Biometric identification: a European priority
Although EU citizens are subject to certain biometric identity obligations, the principal targets of the EU’s biometric identity project so far have been foreign nationals. Biometric identity requirements were initially applied to asylum-seekers and individuals irregularly crossing the EU’s borders, but states expanded their use following the advent of the ‘war on terror’. Two decades later, almost every category of ‘third-country national’ seeking to enter or already present in the EU must have their biometric data captured and recorded in one or another large-scale database.

Asylum-seekers: the first target group

In December 2000, legislation establishing the Eurodac database was adopted. The system was primarily set up to hold the fingerprints of asylum applicants, although from the start it was also used to store the fingerprints of “aliens apprehended in connection with the irregular crossing of an external border.” In 2020, national authorities transmitted almost 645,000 sets of fingerprints to the Eurodac Central System, some for long-term storage and some for comparison to data already held in the system.

From 2015 onwards, with an increasing number of people arriving in the EU to seek asylum, the European Commission began providing additional funds so that ‘frontline’ states, in particular Greece and Italy, could purchase the equipment necessary to ensure biometric enrolment in Eurodac. This was part of the “hotspot approach”, introduced in 2015 as an experimental method for addressing the ‘migration crisis’. The objectives of this included achieving a “100% fingerprinting rate” to feed the Eurodac database that Italy and Greece had, at the time, not been using systematically, with the aim of halting so-called “secondary movements” to the EU’s northern member states. So far, it has not worked, and secondary movements remain high on the EU’s agenda – yet there was a high human cost. In the hotspots, human rights were subordinated to the registration of biometrics and control mechanisms in an uncompromising fashion.

In 2016, the Commission published proposals to expand the system. Under these plans, the age limit for data collection would be lowered from 14 to six years old and, alongside fingerprints, Eurodac would store biographic information and facial images – the latter to “prime the system for searches to be made with facial recognition software in the future,” according to the European Commission. Data would also be stored, for five years, on “third-country nationals or stateless persons found illegally staying in a member state”. The aim is to transform Eurodac into a database “for wider migration purposes,” with a key goal being to increase the number of deportations.

---

2. Ibid.
7. Ibid.
8. Ibid.
databases-for-deportations/

---

**Table 1: Timeline of EU biometric identification legislation**

<table>
<thead>
<tr>
<th>Year</th>
<th>Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Adoption of Eurodac legislation requiring biometric registration of asylum-seekers</td>
</tr>
<tr>
<td>2004</td>
<td>Legislation introducing biometric passports for EU citizens approved; nationals of countries that do not require a visa to enter the EU must also have a biometric passport meeting the same standards</td>
</tr>
<tr>
<td>2006</td>
<td>Second-generation Schengen Information System introduces biometric alerts on refusal of entry or stay in the Schengen area</td>
</tr>
<tr>
<td>2008</td>
<td>Legislation on biometric residence permits for foreign nationals approved</td>
</tr>
<tr>
<td>2008</td>
<td>Legislation on biometric visa applications approved</td>
</tr>
<tr>
<td>2017</td>
<td>Legislation on Entry/Exit System, a biometric border crossing registration database, approved</td>
</tr>
<tr>
<td>2018</td>
<td>New Schengen Information System legislation mandates the inclusion of deportation orders in the database, which may include fingerprints and photographs</td>
</tr>
<tr>
<td>2019</td>
<td>‘Interoperability’ legislation approved</td>
</tr>
</tbody>
</table>
Less than a year after the original Eurodac legislation was adopted, the EU approved new security standards for residence permits and visas, with the aim of preventing identity and document fraud. However, by this point, the political context had shifted significantly, following the 11 September 2001 attacks in the USA and the advent of the ‘war on terror’. The 2004 standards only included ‘traditional’ security features – watermarks, holograms and so on – and governments “made it clear that they [were] in favour of including biometric identifiers in the visa and the residence permit for third country nationals in order to establish a more reliable link between holder, passport and visa.”

The Commission responded with a plan that also covered EU citizens’ passports: on the one hand, to meet US requirements for “biometric elements in passports of citizens of countries granted a visa waiver from 26 October 2004,” and on the other, to meet the joint US-EU goal of “worldwide interoperability” in the use of biometrics “to combat terrorism and illegal immigration.” At the same time, the EU funded a research project aimed at supporting “the consistent implementation of next generation European digital passport.”

Legislation requiring the addition of biometrics to EU citizens’ passports (a photograph and two fingerprints) was approved in 2004, to residence permits (two fingerprints and a photograph) in April 2008, and to short-stay visas (ten fingerprints and a photograph) in July 2008. By the end of 2019 the Visa Information System, a database containing data on short-stay Schengen visa applications, was able to hold up to 100 million visa files, although the actual number held in the system is not published. At the same time, almost 20 million valid residence permits were in circulation. Data on the number of EU member state biometric passports in circulation is not available.

The push for the biometric registration of foreign nationals did not end there. In 2006, legislation upgrading the Schengen Information System (SIS) was approved. This ensured that alerts in the database “issued in respect of third-country nationals for the purpose of refusing entry and stay” could contain both fingerprints and photographs, alongside a wealth of other information. In 2018 the system was further extended, and member states are now obliged to add removal (i.e. deportation) orders to the database. As with alerts on refusal of entry or stay, these may contain fingerprints and photographs, alongside other personal data.

Following the 2006 upgrade of the SIS, politicians, officials and industry representatives began extolling the virtue of “smart borders”. In 2008, the European Commission published proposals aimed at digitising EU border controls. These were subsequently withdrawn, before being updated and reintroduced in 2013. Amongst them was a proposal for an Entry/Exit System (EES), for which legislation was approved in 2017. The EES will be used to capture a photograph, four fingerprints and other data from foreign nationals who do not require a visa to enter the EU, with the aim of automatically generating lists of those who stay longer than permitted. This is intended to better assist the authorities in tracking down and expelling ‘ overstayers’.

By the mid-2010s the EU was either operating, or had mandated the construction of, an array of databases containing biometric data that could be used to verify the identity of foreign nationals in a wide range of different administrative situations – from asylum seekers to foreign residents, visa-holders and migrants from non-visa obliged states. Nevertheless, officials had a more ambitious plan in the works – to transform the data ‘silos’ holding this information into an interconnected system, under the moniker of ‘interoperability’.

Announcing the legal proposals in December 2017, the European Commission said:

“Over the past three years, threats to internal security have evolved and are still very much in evidence, as demonstrated by the series of terrorist attacks in several Member States and the increase in irregular crossings of the EU’s external borders. These challenges have brought into sharper focus the urgent need to strengthen the EU’s information tools for security, border and migration management.”

Statewatch Director Emeritus, Tony Bunyan, highlighted the problem with this justification in 2018:

“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 institutionalised state racism.”


14 https://cordis.europa.eu/project/ST/507974


The fact that terrorism and migration have little, if anything at all, to do with one another, has not deterred the proponents of interoperability from pressing ahead. Nor is there any demonstration that foreign nationals pose more of a security threat than EU citizens, raising the question of whether the push for ‘interoperability’ is taking place because it is objectively necessary, or simply because it is now technically possible.

The initial push for the plan came from Germany, where the authorities established a Central Register on Foreigners (Ausländerzentralregister) following the ‘migration crisis’ of 2015. It stores wide ranging information and access is expanding to an ever longer list of authorities. The EU’s plan involves centralising “identity data” – photos, fingerprints, names, nationalities and information on travel documents – taken from five different large-scale EU databases. This data is to be placed in a system called the Common Identity Repository (CIR), able to hold up to 300 million records.

Access to the system will be permitted under Article 20 of the interoperability rules, which allows for searches by “a police authority” using “the biometric data of that person taken live during an identity check, provided that the procedure was initiated in the presence of that person.” The CIR will also be connected to an automated Multiple-Identity Detector, which will run cross-checks looking for matching data any time a new file is created in an EU database.

One aim of this initiative is to facilitate identity checks by law enforcement authorities, as part of a drive to tackle identity fraud and to increase the number of deportations. Access to the system will be permitted under Article 20 of the interoperability rules, which allows for searches by “a police authority” using “the biometric data of that person taken live during an identity check, provided that the procedure was initiated in the presence of that person.” The CIR will also be connected to an automated Multiple-Identity Detector, which will run cross-checks looking for matching data any time a new file is created in an EU database.
The CIR will be accessible via fixed access points at border crossings, police stations and consulates, amongst other places, but the intention is also for officials to make use of the system via mobile biometric identification technologies. These are typically handheld devices that can capture biometric data from an individual (typically, their fingerprint or face, although other means of biometric identification exist) and automatically compare it against a database or watchlist.

There is a substantial market for these devices, with companies large and small keen to provide state authorities with the latest tools for individual identification. “More than 20 countries in Europe” use hardware produced by Germany company DERMALOG, “for government applications such as National Registration, Border Control and Refugee Registration.” Thales boasts of “more than 200 biometric deployments in 80 countries, leveraging strong biometric authentication and identification worldwide for customers at all government levels.” NEC claims to be “the world’s leading supplier of fingerprint biometrics for both law enforcement and identity management applications,” having spent “about half a century in developing the most efficient and accurate fingerprint identification technology.”

Nevertheless, the acquisition and use of mobile biometric technologies is considered by the European Commission to be one of the more difficult aspects of the interoperability project: “The expected complexity lies with the Member States needing to purchase and customise handheld biometric terminals and connect them to their national police systems,” a process that requires substantial organisational and procedural changes (see section Police technology networks of this report). Legal changes may also be required, in order to adapt national law with the requirements of Article 20, although as of summer last year only 13 of the states participating in the interoperability initiative (less than half of the total) had finished assessing whether any changes were necessary.

As for acquiring the technology needed to step up biometric identity checks, the situation differs widely from one state to another. Freedom of information requests filed by Statewatch for this report sought to establish the state of play in France, Italy and Spain, but they remained unanswered by the time of publication. Among civil society experts and researchers questioned by Statewatch, there was limited knowledge of current plans, specifically with regard to the implementation of the interoperability initiative.

Despite the lack of comprehensive and accessible public information on implementation, records indicate that states are taking steps in this direction. In 2019 the French police were granted the power to check, “on the basis of the fingerprints of a foreigner without a permit registered in AGDREF [the file of foreign nationals present in France].” The administration has spent €7.5 million on equipment for the AGDREF database and various types of fingerprint readers since 2017, and in February last year, the interior ministry published a call for information seeking an “AI-based solution” allowing the cross-matching of identity across multiple databases on the basis of a fingerprint. It also sought “biometric sensor solutions” that would allow the authorities to “meet new needs,” including “mobile fingerprint capture... preferably via a smartphone/tablet... or even more preferably from the camera of a smartphone/tablet.”

This is already happening in Germany: in Hamburg, a mobile app lets police scan fingerprints using a smartphone. The Dutch police, meanwhile, appear to be pioneers in this field. In 2011, the authorities began providing mobile fingerprint scanning technology to the police, a move “primarily intended for more intensive checks on illegal aliens,” according to the newspaper Trouw. An EU-funded programme in Greece seeks to equip hundreds of officers with handheld fingerprint and facial scanners with the aim of targeting irregular migrants.

In 2014, the Spanish authorities used over €300,000 from the EU’s Internal Security Fund to equip officers of the Guardia Civil with “portable data terminals, with which the databases can be accessed remotely and in real time,” to be deployed “in areas of a high risk of irregular immigration.” The Danish and Swedish authorities have also used the Internal Security Fund to purchase mobile identification devices to aid in the implementation of the Entry/Exit System, while the Romanian authorities have purchased “mobile control devices” to ease access to the Schengen Information System.
There thus appears to be a patchwork of different national initiatives on mobile identification, some of which are related to the implementation and use of EU databases, and others which are not. Once mobile biometric identification devices are in use, however, they can then be connected to further systems and data sources. There are undoubtedly further projects and deployments beyond those uncovered during the research for this report; and there will likely be many more to come as the implementation of the interoperability initiative, and national plans seeking to increase mobile biometric controls, continue. There is a need for increased investigation into and scrutiny of these projects, to ensure that – at the very least – the authorities meet their obligations to carry out meaningful equality and data protection impact assessments, and put adequate safeguards in place around identity checks by police and immigration authorities.

Asylum-seekers: test subjects for ‘interoperability’

The Spanish state has substantially developed its biometric systems in recent years. Upon arrival at Spain’s borders, people claiming asylum have their information recorded in an “integral system for the management of applications under international protection,” or SIGESPI. This is managed by the company GMV.\(^47\) Ironically, the company is also responsible for management of the European Border Surveillance System, EUROSUR,\(^48\) designed in part to try to keep asylum-seekers away from EU territory.\(^49\)

Demonstrating the trend towards ‘interoperability’ at national level, the system is connected to a multitude of other databases including police, criminal records, civil registration and visa systems, for the purpose of conducting background checks on asylum-seekers. Human rights organisation Novact have noted that “the centralisation and interoperability between databases poses grave risks for people’s privacy.”\(^50\) Whether at local, national, regional or international level, the more data that is interconnected and the greater the number of access points, the more likely it is that data will be accessed and used illegally, particularly if the data protection authorities responsible for supervision and inspection do not have the resources needed to carry out their tasks.

Indeed, Spain’s ‘guardarmerie’ force, the Guardia Civil, were systematically (and illegally) accessing SIGESPI between 2013 and 2014 for the purpose of criminal investigations, logging some 1.5 million searches in that period. The practice was denounced in 2015 by the Policía Nacional, who control the system.\(^51\) Granting police forces access to systems holding data on asylum-seekers and other foreign nationals for the purpose of criminal investigations is now standard practice at EU level, following the adoption of controversial changes to Eurodac in 2013.\(^52\) In practice, this has the effect of criminalising these groups: if similar databases storing information gathered from citizens do not exist, there is no way they can be subject to the same level of police scrutiny.

Furthermore, the growing number of authorities granted access to both national and EU systems increases the possibilities for illegal access to data, whether on an individual or institutional level. While legislation generally contains safeguards requiring controls on and the logging of access to data, ensuring compliance implies a substantially increased workload for national data protection authorities, many of whom are already short on resources and personnel. The legal and practical complexity of interoperable systems further compounds the problem.
3. Funding for biometric technologies
The EU is one of the largest providers of public funding for “research and innovation” in the world, and substantial amounts of money have gone into developing the technologies needed to implement its biometric identity programme. The current EU research programme, Horizon Europe, runs from 2021 until 2027 and has a total budget of some €95 billion. This will provide funding for projects and activities on medical research, the environment, climate change and transport, amongst other things. One segment of the programme, worth €1.6 billion, is directed towards security, under the heading ‘Civil Security for Society’.

Biometrics and security research

The Civil Security for Society theme is the latest iteration of the long-standing European security research programme, which has been in place since 2004 and was formally integrated into the broader research agenda from 2007 onwards. It is geared towards developing new technologies and techniques for dealing with issues such as crime, terrorism, border control, disaster management and response, and cybersecurity. It primarily does so by funding the activities of consortia – made up of private companies, public bodies, research institutes or higher education institutions – that are formed to carry out particular research projects.

Under the security heading these have looked at, for example, the development of new video surveillance techniques, networks of different sensors that can be mounted on drones and used for border control, or communications tools for emergency services. National authorities often also have their own security research programmes – for example, the German government has funded research aiming towards “a technical solution that enables identity authentication for mobile use by police and relevant authorities”. Biometric technology has long been a focal point of the security research programme, although EU research funding for biometrics goes back some way further. During the late 1990s and early 2000s, biometrics funding largely came from the IT theme of the fifth and sixth research framework programmes (1998-2002 and 2002-2006, respectively) and was directed towards potential commercial or healthcare applications.

From 2007 onwards, however, the security theme became by far the most significant source of such funding, and the number of projects funded skyrocketed – a clear demonstration of the central role granted to biometric identity in the EU’s security agenda. In total, the EU has awarded over €290 million in public funding to biometric research and development projects since 1998, with almost 40% of those projects primarily concerned with issues of ‘public security’ – law enforcement, border control and other such topics. Projects have examined generic uses of the technology (for example, “innovative technology to take fingerprint images” or systems for testing and certifying different biometric systems) as well as applied uses of biometrics, in particular in the field of border control.

Of the 27 biometric research projects funded between 2007 and 2013, 11 (41%) were part of the security research programme. The proportion grew under Horizon 2020, in which 27 of the 57 biometrics research projects (47%) came under the security banner (see Chart 3). Security-focused projects also received more funding than those researching ways to deploy biometrics in other fields: during FP7, security projects received 62% of the funds directed towards biometrics, an amount that decreased to 60% in Horizon 2020, as shown in Table 2.

<table>
<thead>
<tr>
<th>Horizon 2020 (2014-20)</th>
<th>Total biometrics funding</th>
<th>Total no. of projects</th>
<th>Security biometrics funding</th>
<th>No. of security projects</th>
<th>Security spending, % of total</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP6 (2002-06)</td>
<td>€32,843,791</td>
<td>13</td>
<td>€15,249,995</td>
<td>4</td>
<td>46%</td>
</tr>
<tr>
<td>Total</td>
<td>€290,347,73</td>
<td>113</td>
<td>€163,464,515</td>
<td>46</td>
<td>56%</td>
</tr>
</tbody>
</table>

Table 2: Biometric funding in EU research programmes, 1998-2020

---

58 All the figures provided in this section are based on an analysis of CORDIS data available on the EU’s Open Data Portal, https://data.europa.eu/euodp/en/data/
Chart 1: EU funding for biometric research, 1998 – 2020

This chart shows the amount of research funding dedicated to biometric research overall, and the amount dedicated to public security research projects.

Chart 2: Number of EU-funded biometric research projects, 1998 - 2020.

This chart shows the number of projects dedicated to research on biometrics overall, and the number of projects related to public security.
Chart 1: EU funding for biometric research, 1998-2020. This chart shows the amount of research funding dedicated to biometric research overall, and the amount dedicated to public security research projects.

Chart 2: Number of EU-funded biometric research projects, 1998-2020. This chart shows the number of projects dedicated to research on biometrics overall, and the number of projects related to public security.

**Chart 2: Number of EU-funded biometric research projects, 1998-2020.**
This chart shows the number of projects dedicated to research on biometrics overall, and the number of projects related to public security.
Chart 3: Average funding per biometric research project by type of institution, FP7 and H2020.

This chart shows that the average amount of funding received by private companies, higher education institutions and research institutes has consistently been higher for public security projects than for other types of biometric research projects.
Chart 3: Average funding per biometric research project by type of institution, FP7 and H2020.

This chart shows that the average amount of funding received by private companies, higher education institutions and research institutes has consistently been higher for public security projects than for other types of biometric research projects.

Chart 4: Difference between average received per project, compared to overall average funding per project.

This chart shows whether funding different types of institutions received more or less funding from the FP7 and H2020 research programmes than the average amount provided (the average is represented by the central line, marked €-). For example, public bodies always received significantly less than the average, and private companies always received more than the average for participating in public security projects.
Advancing state and industrial interests

Private companies, along with state-backed research institutes and higher education institutions, have been the most significant financial beneficiaries of research into biometrics, a fact that is particularly pronounced in the security research programme. Private companies received almost €53 million (43%) of the total biometric research funding in FP7, but this increased to 49% of the funding awarded as part of the security theme (€37.5 million). In contrast, they received only 34% of the funding (€15.4 million) awarded to biometrics research under other themes. In Horizon 2020 the picture was similar: private companies received 49% of all biometric research funding (€55.6 million). This amount increased to 57% (€38.9 million) under the security theme; but dropped to 36% of funding awarded (€16.6 million) under other research themes (as shown in Table 5). The security theme has also generally provided a greater average amount of funding under the security heading than the programme overall, with regard to private companies, higher education institutions and research institutes (see Charts 3 and 4).

A small number of these research projects have sought to examine the ethical and legal implications of biometric technologies for policing and border control. However, the vast majority have aimed to find new means and modes of biometric identification and authentication (including gait recognition and speech analysis alongside the more ‘traditional’ facial and fingerprint recognition), and more efficient ways for the authorities to make use of them. It must also be noted that even if a research project is ostensibly geared towards the use of biometrics for commercial, health, or otherwise more ‘benign’ purposes than for policing or immigration, it is still designed to further the use of advanced techniques of data processing and surveillance, and the basic technology itself may very well be adapted for other purposes.

<table>
<thead>
<tr>
<th>Country</th>
<th>H2020</th>
<th>FP7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>€17,249,314</td>
<td>€9,326,356</td>
<td>€26,575,671</td>
</tr>
<tr>
<td>Spain</td>
<td>€15,536,605</td>
<td>€10,556,553</td>
<td>€26,093,158</td>
</tr>
<tr>
<td>Germany</td>
<td>€12,833,926</td>
<td>€12,863,261</td>
<td>€25,697,187</td>
</tr>
<tr>
<td>France</td>
<td>€9,307,630</td>
<td>€12,834,126</td>
<td>€22,141,755</td>
</tr>
<tr>
<td>Italy</td>
<td>€7,668,215</td>
<td>€11,691,939</td>
<td>€19,360,154</td>
</tr>
<tr>
<td>Greece</td>
<td>€8,120,425</td>
<td>€5,774,133</td>
<td>€13,894,558</td>
</tr>
<tr>
<td>Netherlands</td>
<td>€4,074,005</td>
<td>€5,316,198</td>
<td>€9,390,204</td>
</tr>
<tr>
<td>Belgium</td>
<td>€5,061,878</td>
<td>€3,785,362</td>
<td>€8,847,240</td>
</tr>
<tr>
<td>Austria</td>
<td>€4,513,025</td>
<td>€3,477,791</td>
<td>€7,990,816</td>
</tr>
<tr>
<td>Finland</td>
<td>€1,137,943</td>
<td>€6,734,474</td>
<td>€7,872,416</td>
</tr>
<tr>
<td>Norway</td>
<td>€4,782,978</td>
<td>€2,497,570</td>
<td>€7,280,548</td>
</tr>
<tr>
<td>Switzerland</td>
<td>€2,025,986</td>
<td>€4,981,970</td>
<td>€7,007,956</td>
</tr>
<tr>
<td>Portugal</td>
<td>€3,322,625</td>
<td>€2,767,006</td>
<td>€6,089,631</td>
</tr>
<tr>
<td>Romania</td>
<td>€2,003,408</td>
<td>€3,245,933</td>
<td>€5,249,341</td>
</tr>
<tr>
<td>Poland</td>
<td>€2,438,817</td>
<td>€2,418,245</td>
<td>€4,857,063</td>
</tr>
<tr>
<td>Sweden</td>
<td>€979,958</td>
<td>€3,555,097</td>
<td>€4,535,055</td>
</tr>
<tr>
<td>Denmark</td>
<td>€2,690,857</td>
<td>€ -</td>
<td>€2,690,857</td>
</tr>
<tr>
<td>Ireland</td>
<td>€1,580,126</td>
<td>€1,078,372</td>
<td>€2,658,498</td>
</tr>
<tr>
<td>Iceland</td>
<td>€1,405,750</td>
<td>€1,164,620</td>
<td>€2,570,370</td>
</tr>
<tr>
<td>USA</td>
<td>€ -</td>
<td>€2,321,915</td>
<td>€2,321,915</td>
</tr>
</tbody>
</table>

Table 3: Distribution of biometric research funding by state (top 20)

The extent to which the security research programme itself is a success is, however, open to question. The programme is ultimately meant to contribute to the development, testing, acquisition and sharing of technologies, techniques, knowledge and products, with the aim of boosting the European security industry and ultimately providing “increased security of European citizens.” However, official evaluations of both FP7 and H2020 have reported low numbers of intellectual property registrations and academic publications; and the interim evaluation of H2020 noted “consortium members can be reluctant to release their [intellectual property] to enable the commercialization of the final product.” The report went on to cite an example:

“End-users [i.e. border guards] explain that European tax-payers pay but only get a demonstration product or prototype at the end of the project, with limited, if any, take-up. In one project, FRONTEX and national border agencies would have liked to use the technology, but were asked for €150,000 to use the platform.”

Nevertheless, the EU has clearly played a role in establishing and maintaining collaborative networks of small and large companies, research and educational institutions and public authorities working to develop and deploy new biometric identification and verification technologies. This is set to continue in the latest iteration of the security research programme: the 2021-22 work programme includes topics on “modern biometrics used in forensic science and by police”; “improved border checks for travel facilitation across external borders and improved experiences”; and “enhanced security of, and combating the frauds on, [sic] identity management and identity and travel documents.”

Closer links are also being forged with the intended “end-users” of new technologies. EU border agency Frontex has taken on an increased role in the programme following the entry into force of its 2019 mandate, and

---

**Table 4:** Top 20 recipients of biometric research funding, FP7 (2007-13) and H2020 (2014-20)

<table>
<thead>
<tr>
<th>Institution</th>
<th>FP7 funding</th>
<th>H2020 funding</th>
<th>Total funding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idemia Identity &amp; Security (France)</td>
<td>€7,194,528</td>
<td>€2,259,944</td>
<td>€9,454,471</td>
</tr>
<tr>
<td>Fraunhofer Institute (Germany)</td>
<td>€5,502,548</td>
<td>€2,683,323</td>
<td>€8,185,870</td>
</tr>
<tr>
<td>Austrian Institute of Technology</td>
<td>€4,332,493</td>
<td>€666,919</td>
<td>€4,999,412</td>
</tr>
<tr>
<td>Vision Box (Portugal)</td>
<td>€2,552,437</td>
<td>€2,093,700</td>
<td>€4,646,137</td>
</tr>
<tr>
<td>Catholic University of Leuven (Belgium)</td>
<td>€3,091,779</td>
<td>€1,329,280</td>
<td>€4,421,059</td>
</tr>
<tr>
<td>University of Reading (UK)</td>
<td>€1,430,943</td>
<td>€2,515,304</td>
<td>€3,946,247</td>
</tr>
<tr>
<td>Information Technologies Institute (Greece)</td>
<td>€3,032,426</td>
<td>€818,871</td>
<td>€3,851,297</td>
</tr>
<tr>
<td>Idiap Research Institute (Switzerland)</td>
<td>€2,859,079</td>
<td>€562,553</td>
<td>€3,421,632</td>
</tr>
<tr>
<td>University of Lancaster (UK)</td>
<td>€376,276.91</td>
<td>€2,953,573.15</td>
<td>€3,329,850.06</td>
</tr>
<tr>
<td>Atos (Spain)</td>
<td>€1,932,744.18</td>
<td>€1,914,166.88</td>
<td>€3,846,911.06</td>
</tr>
<tr>
<td>Defence Research Institute (Sweden)</td>
<td>€2,933,183.50</td>
<td>€-</td>
<td>€2,933,183.50</td>
</tr>
<tr>
<td>Veridos (Germany)</td>
<td>€417,705.50</td>
<td>€2,324,075.00</td>
<td>€2,741,780.50</td>
</tr>
<tr>
<td>Alternative Energies and Atomic Energy Commission (France)</td>
<td>€1,443,370.00</td>
<td>€1,223,807.50</td>
<td>€2,667,177.50</td>
</tr>
<tr>
<td>Thales (France)</td>
<td>€2,097,342.70</td>
<td>€474,936.25</td>
<td>€2,572,278.95</td>
</tr>
<tr>
<td>Gjovik University College (Norway)</td>
<td>€2,396,193.00</td>
<td>€-</td>
<td>€2,396,193.00</td>
</tr>
<tr>
<td>EURECOM (France)</td>
<td>€646,175.00</td>
<td>€1,717,632.83</td>
<td>€2,363,807.83</td>
</tr>
<tr>
<td>Autonomous University of Madrid (Spain)</td>
<td>€1,314,584.00</td>
<td>€1,003,619.52</td>
<td>€2,318,203.52</td>
</tr>
<tr>
<td>Zwipe (Norway)</td>
<td>€-</td>
<td>€2,297,400.00</td>
<td>€2,297,400.00</td>
</tr>
<tr>
<td>Indra (Spain)</td>
<td>€1,991,201.37</td>
<td>€222,250.00</td>
<td>€2,213,451.37</td>
</tr>
</tbody>
</table>

---

63 Ibid.

67 Recital 11, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol’s cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol’s role on research and innovation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0796


<table>
<thead>
<tr>
<th>Private companies</th>
<th>Public bodies</th>
<th>Higher education institutions</th>
<th>Research institutes</th>
<th>Other</th>
<th>Total in €</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount in €</td>
<td>% of total</td>
<td>Amount in €</td>
<td>% of total</td>
<td>Amount in €</td>
<td>% of total</td>
</tr>
<tr>
<td><strong>FP7 total</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>52,966,852</td>
<td>43</td>
<td>€2,968,732</td>
<td>2</td>
<td>32,665,983</td>
<td>27</td>
</tr>
<tr>
<td><strong>H2020 total</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>55,573,383</td>
<td>49</td>
<td>3,397,837</td>
<td>3</td>
<td>36,787,747</td>
<td>32</td>
</tr>
<tr>
<td><strong>FP7 security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37,534,411</td>
<td>49</td>
<td>2,428,208</td>
<td>3</td>
<td>15,400,855</td>
<td>20</td>
</tr>
<tr>
<td><strong>H2020 security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38,928,437</td>
<td>57</td>
<td>2,862,799</td>
<td>4</td>
<td>14,767,350</td>
<td>22</td>
</tr>
<tr>
<td><strong>FP7 other</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15,432,441</td>
<td>34</td>
<td>540,524</td>
<td>1</td>
<td>17,265,128</td>
<td>38</td>
</tr>
<tr>
<td><strong>H2020 other</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16,644,945</td>
<td>36</td>
<td>535,038</td>
<td>1</td>
<td>22,020,397</td>
<td>48</td>
</tr>
</tbody>
</table>

Table 5: Funding distribution by institution type for biometric research in FP7 (2007-13) and H2020 (2014-20)
Funding 'smart borders'

It was through the FP7 research and development programme that the EU sought to develop the technology needed for its ‘smart borders’ initiative: projects such as ABC4EU, FASTPASS, FIDELITY and MOBILEPASS worked on the development of automated border control gates and swift, reliable, mobile biometric acquisition and verification technologies. The most recent overall evaluation of the research programme highlighted the MOBILEPASS project as a success story:

“The equipment developed enables authorities to perform contactless fingerprint acquisition, encompassing the whole chain from fingerprint data obtained from passports up to contactless verification. This innovative solution also has significant added value, as the border checks can be executed in a more comfortable, fast and secure way.”

The Spanish state has been an enthusiastic adopter of new biometric border technologies, with funds drawn from a variety of EU and national budgets. The country has shown particular interest in the “smart borders” that will underpin the Entry/Exit System, in which all businesspeople, holidaymakers and other visitors to the EU will have their biometrics stored and border crossings recorded. The €18 million ABC4EU (automated border control) project was coordinated by Spanish security company Indra, and five of the project’s 18 participants were based in Spain. ABC gates can use facial recognition, iris recognition, fingerprints or other biometric traits to match information from an individual either to their travel document, to data registered in a central database, or to both.

Ironically, despite claims from proponents that ABC systems will ensure convenience and speed at border crossings, an initial 2015 pilot project at the Spain-Gibraltar frontier led to queues so large that it was halted after two hours. The gates will, however, provide a key site for the collection and verification of biometric and other data. The same border recently worked host to a Frontex-supported trial of the EES, with the agency announcing the system will “change the way we cross borders and help protect the security of European citizens centralising [sic] the information on border crossings.” The company Everis will receive almost €6.4 million to construct the Spanish national system and connect it with the central EES database, and a €20 million tender to supply equipment for Spanish border crossing points closed to bids at the end of last year.
4. Police technology networks
Beyond the security research programme, an array of different actors has used EU funding and fora to advance plans for increased mobile biometric identity controls. In 2008, the EU's Joint Research Centre hosted a conference that brought together some 70 police and immigration officials to discuss “their views and experiences based upon initial trials on the use of mobile devices for identification and authentication of individuals.” The aim was to launch “a discussion on mobile identification which would address important issues such as best practices in processes and procedures, technical standards, their evaluation in a pan-European harmonised way and interoperability among the different solutions available or adopted.”

This led to the establishment of the European Mobile Identification Interoperability Group (e-MOBidIG), which was led by Frank Smith, a UK Border Agency official. By 2011, it had five sub-groups and industry representatives were regularly invited to its meetings. In March 2010, responses to a questionnaire circulated amongst the group’s members showed that eight EU member states (those that responded) were using or testing mobile ID devices, and that six were using such devices for border control purposes. The group was eventually subsumed into a more extensive entity – the European Network of Law Enforcement Technology Services (ENLETS).

ENLETS also began life in 2008, on the back of an idea put forward by the French delegation to the Council of the EU’s Police Cooperation Working Party for “an informal network of heads of departments responsible for implementing new technologies in police departments.” It took some time for the network to gain momentum, but by 2012 a “core group” had been established and had agreed upon a number of priority areas, including various surveillance technologies (automatic number plate recognition, covert listening and drones) and non-lethal weapons, amongst other things. In 2013 ENLETS received high-level political approval from the Justice and Home Affairs Council and the European Commission began to provide funding, which has continued ever since.

When e-MOBidIG became part of ENLETS, it was transformed into a sub-group known as the ‘ENLETS mobile group’. In 2017, the mobile group produced a report that declared a “turning point” had been reached in terms of the possibilities offered to police by new technologies. “Mobile technology is now a disruptive force for reform,” said the document, which would make it possible for officers to have instant, 24/7 access to data, profiles, images, videos and biometrics on everybody stopped, checked or under surveillance.

This would primarily be through mobile access to EU databases, said the report, requiring “new rules for the way national and European systems function” – precisely the type of rules introduced by the ‘interoperability’ initiative, the proposals for which were published the month prior to the ENLETS report. The report also highlighted the importance of “thorough ID checks as a mandatory first step in any process,” although it underscored that major, complex organisational and procedural changes would be required to implement its vision of ‘mobile policing’:

“Implementing mobile solutions in policing on a large scale is a major undertaking... it involves an integral change process on most aspects of the organization and as such strategic level priority is called for.”

Whether any immediate action was taken to encourage the “integral change process” is unknown. However, some years later, in November 2020, a note to the Council’s Working Party on Information Exchange from the German Presidency of the Council demanded a “paradigm shift” that would introduce:

“...a need for a new integrated information architecture for internal security, border management and migration. It should consolidate the capabilities of digital technologies and available information and provide an extended and powerful tool for practitioners, increasing the efficiency of their daily work.”

This, the Presidency noted, was being dealt with through the construction and interconnection of new and existing large-scale databases via the interoperability initiative. However, the Presidency also highlighted that for interoperability to achieve “maximum effect,” the data entered into those systems needed to be “of very high quality,” and users of the systems needed “timely, secure and comprehensive access” to it. This would require:

“...a new eco system of devices and solutions for the acquisition of raw data and access to information for the purposes of internal security, border management and migration as well as the further strengthening of cybersecuri...”

The adoption of common technical standards and procedures across the member states was identified as the best way of ensuring that data of sufficient quality was entered into the systems, and then made available and accessed in a uniform way. The Working Party on Information Exchange -

eu-funding-for-network-developing-surveillance-intelligence-gathering-and-remote-vehicle-stopping-tools/


thus adopted a “roadmap”,\textsuperscript{90} intended to guide the adoption of standards for:

- biometric data quality;
- alphanumeric data quality;
- devices for the acquisition of raw biometric data; and
- mobile devices and solutions.

The Portuguese Presidency followed up with an ‘Action Plan for the implementation of the Roadmap’.\textsuperscript{91} A panoply of agencies, working parties and institutions are involved, with the EU’s agency for justice and home affairs databases, eu-Lisa,\textsuperscript{92} coordinating the work. Activities include attempts to shape international technical standards to encourage companies to develop products compliant with the EU’s requirements;\textsuperscript{93} for EU agencies to develop training curricula on the acquisition and use of biometrics; and the creation of a “reference catalogue of devices and solutions for the acquisition of data and access to information in the central systems (SIS, VIS, EES, ECRIS-TCN, EURODAC).”

This catalogue will inform national authorities of relevant equipment available for police officers, border guards and others seeking to enter or access data in EU information systems, and will cover:

- fixed and hand-held facial image scanners;
- fixed and hand-held fingerprint and palm scanners;
- “other biometric identification solutions that may become relevant in the future”;
- document readers and scanners;
- “mobile solutions for access to information (e.g. handheld devices used by border guards and law enforcement authorities)”.\textsuperscript{94}

Frontex, Europol, the European Agency for Asylum, national authorities, the Commission’s DG HOME and the EU Joint Research Centre are to support the creation of the catalogue by providing information to eu-Lisa. They are also tasked with carrying out surveys, studies and analyses on “business and operational requirements,” the “impact and outcomes of the ongoing initiatives concerning the future of travel,”\textsuperscript{95} and turning “business requirements” on the “strategic, tactical and operational level into solution-based requirements for new systems, initiatives and recasts [legal reforms].”\textsuperscript{96}

Underneath the jargon, this last point demonstrates that this is not merely a technical exercise to aid the implementation of legal and policy measures that have been agreed by EU institutions – it is also intended to create a way for the “requirements” of state agencies and institutions to feed back into new policies and laws. In this regard, it should be underscored that while “roadmaps” and “action plans” may be useful ways for a diverse array of actors and organisations to coordinate their activities, the fact that they tend to be kept hidden from public view and intended only for discussion amongst a limited set of officials does not provide much room for democratic scrutiny or deliberation.


\textsuperscript{91} Council of the EU, ‘Action Plan for the implementation of the Roadmap for standardisation’, Council document 9105/21, 16 June 2021 (not currently public)

\textsuperscript{92} The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice.

\textsuperscript{93} The report notes: “As suggested above, the alignment with the international standards of biometric systems developed and operated by eu-LISA, as well as those used by the Member State authorities, will be essential to ensure high quality of biometric data. Since 2021, along with representatives of several EU Member States, eu-LISA has been involved in the development of the ISO [International Standards Organisation] family of standards on biometrics, by means of a liaison with the ISO standardisation sub-committee ISO/IEC/TC1/SC37. Although expert representatives of a number of EU Member State authorities are already involved in the standardisation work of the aforementioned sub-committee, strengthening the engagement of EU Member States in the standardisation work will help steer the development of international standards in the area of biometrics and on-board specific requirements relevant within the EU context. Elevating EU requirements to the status of international standards could provide additional impetus for the industry to develop technologies and solutions meeting these specific requirements, therefore potentially enhancing competition in the market.”


\textsuperscript{96} Council of the EU, ‘Action Plan for the implementation of the Roadmap for standardisation’, Council document 9105/21, 16 June 2021 (not currently public)
Right data, wrong identity

When it comes to the identification and verification of individuals, the collection of biometric data such as facial images and fingerprint scans is supposed to help deal with the problem of incorrect or incomplete data – by using digitised measurement of physical traits, information can be ‘fixed’ to an individual. However, the fact that vast numbers of people need to use false identities to cross borders and reach safety can lead to them getting ‘stuck’ with that identity.

Since 2019, unaccompanied migrant children in France have been obliged to have biometric and other data registered in a centralised file in order to receive assistance: an instance of what the European Commission once referred to as the “no registration no rights” principle. The official purpose of the system is to “better guarantee the protection of children” and to “fight against the illegal entry and residence of foreigners in France”. However, children who travelled to the EU on a false (adult) passport have been treated as if they were that person, meaning they have not had access to the services and care required for children. Equally, children who refuse to give their fingerprints are, by default, treated as adults.

A number of regional authorities refused to participate in a system they considered as running counter to the best interests of children. The state then cut funding to them. In response, a group of human rights organisations demanded that the government abolish the entire biometric registration system for children, which they argue rests upon a “confusion between child protection and the fight against irregular immigration.”

Thus, data that is erroneously entered (for example, misspelt names or other details), as well as data that is false or misleading (but necessary for the individual concerned to reach safety) are both capable of having negative effects for individuals. This is particularly so given the official deference to data that has been formally registered in one system or another: “There is high trust in information provided in an IT-system, according to public officials, lawyers and experts” a report by the EU’s Fundamental Rights Agency noted.

As Nicholas Chevreux, an asylum lawyer in Germany, told Statewatch: “we can only explain why the registration is wrong, why the data in the database is wrong. But it is extremely difficult, and it’s almost impossible to convince [anyone] that the computer is wrong”.

Moreover, despite the ongoing increase in data collection, individuals rarely exercise their rights to access it to check its veracity and lawfulness. With so many other problems to deal with, individuals in the asylum system are unlikely to seek to correct data held on them, particularly for details like spelling of name, despite the centrality of accurate information to legitimate decision-making. There is of course a tension here: while there is a general legal obligation for personal data processed by public authorities to be accurate and up-to-date, taking this as a starting point in the analysis of a given project or initiative sidesteps questions over the legitimacy of that data-gathering in the first place.
5. Advanced technology, regressive practices
Adding a new technological component to identity checks will do little to rectify this problem. Quite the contrary: it is likely exacerbate it. With authorities seeking to increase the number of deportations, and skin colour treated as a proxy for an individual's immigration status, any attempt to increase the number of identity checks has serious implications for ethnic minority EU and non-EU citizens alike. While there may be safeguards in place – for example, in the EU's data protection laws or in the interoperability legislation itself – these may simply be ignored or insufficient.

Ethnic profiling by police

A 2018 survey of over 5,800 people of African descent in 12 EU member states, carried out by the EU Fundamental Rights Agency (FRA), showed that 24% of respondents had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

By police

A 2018 survey of over 5,800 people of African descent in 12 EU member states, carried out by the EU Fundamental Rights Agency (FRA), showed that 24% of respondents had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

By police

A 2018 survey of over 5,800 people of African descent in 12 EU member states, carried out by the EU Fundamental Rights Agency (FRA), showed that 24% of respondents had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

By police

A 2018 survey of over 5,800 people of African descent in 12 EU member states, carried out by the EU Fundamental Rights Agency (FRA), showed that 24% of respondents had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

By police

A 2018 survey of over 5,800 people of African descent in 12 EU member states, carried out by the EU Fundamental Rights Agency (FRA), showed that 24% of respondents had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

By police

A 2018 survey of over 5,800 people of African descent in 12 EU member states, carried out by the EU Fundamental Rights Agency (FRA), showed that 24% of respondents had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. In Spain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.

Beyond individual perceptions, other data demonstrates the racial disproportionality of police checks. InSpain, the FRA identified in a 2008 survey that 42% of people with irregular status had been stopped by the police in the five years before the survey; and 11% in the 12 months before the survey. Of those stopped in the last 12 months, 44% considered that “the last stop they experienced was racially motivated,” although this perception differed widely between people living in different states, and between men and women.
European Court of Human Rights,\textsuperscript{120} concerning a Pakistani national and Spanish resident, Zeshan Muhammad, may remedy this. Muhammad was stopped with a friend by police in Barcelona in 2013 under suspicion of being in Spain irregularly.\textsuperscript{121} The officer in question used “racially charged language” to explain that the colour of Muhammad’s skin was the reason for the apprehension.\textsuperscript{122} Muhammad filed a complaint that such ethnic profiling violates Spain’s constitution and international treaties. The case was dismissed by both Spain’s high court and the constitutional court, and is now awaiting a hearing in Strasbourg.

The Williams case was followed by some changes in practices. National police in Spain committed to define and prohibit ethnic profiling in identity checks, including measures to record all instances and log the perceived ethnicity of those apprehended.\textsuperscript{123} Other initiatives have also sought to improve the situation. A pilot project undertaken by the Platform for Police Diversity Management (Plataforma por la Gestión policial de la Diversidad) brought together police associations and anti-discrimination organisations to promote best practices for police in the realm of non-discrimination.\textsuperscript{124} Under this pilot, “stop forms” were adopted. Records of stops across five Spanish police departments demonstrated that the act of recording stop and search activities led to fewer discriminatory checks.\textsuperscript{125} However, the national police body has shown little interest in following suit.\textsuperscript{126} In localities where the model has been introduced, lack of feedback from senior officials has contributed to lower rates of improvement, while in Girona, police officers even increased apprehensions of non-white people out of frustration with the new policy.\textsuperscript{127}

In France, as in Spain, there is no official collection of data on the ethnicity of people stopped for identity checks. An Open Society Initiative study conducted in 2009 identified that people were six times more likely to be stopped if they were black, and almost eight times more likely if they appeared to be Arab.\textsuperscript{128} A former French ombudsman has said that “compared to the general population and all other things being equal, young men in France, who are perceived as Arab/Maghrebin or Black, are 20 times more likely to be subjected to identity checks than others”.\textsuperscript{129} The UN High Commissioner for Human Rights singled out France in relation to discriminatory police stops in June 2021.\textsuperscript{130}

The following month, six civil society organisations filed a class action lawsuit demanding structural reforms and measures to end discrimination in police practices, including tighter regulation, improved police training and reporting around identity checks and their impact.\textsuperscript{131} Previously, in a 2016 case, the Court of Cassation recognised state responsibility for a case involving discriminatory identity checks of three people, treatment that amounted to “gross misconduct”.\textsuperscript{132} The court underlined the fact that checks were undertaken for one and a half hours, targeted members of “visible minorities”, and the state failed to show that there were objective reasons to justify the checks.

In Italy, ethnographic studies indicate similar problems. The academic Martina Tazzioli has undertaken extensive fieldwork in the border region between Italy and France – an internal border between two EU member states at which there is now a push to increase identity checks (an issue explained further below). When the Arab Spring uprisings resulted in a spike in irregular departures of people across the Mediterranean, Tazzioli found that:


disparities to promote best practices for police in the realm of non-discrimination.\textsuperscript{124} Under this pilot, “stop forms” were adopted. Records of stops across five Spanish police departments demonstrated that the act of recording stop and search activities led to fewer discriminatory checks.\textsuperscript{125} However, the national police body has shown little interest in following suit.\textsuperscript{126} In localities where the model has been introduced, lack of feedback from senior officials has contributed to lower rates of improvement, while in Girona, police officers even increased apprehensions of non-white people out of frustration with the new policy.\textsuperscript{127}

In France, as in Spain, there is no official collection of data on the ethnicity of people stopped for identity checks. An Open Society Initiative study conducted in 2009 identified that people were six times more likely to be stopped if they were black, and almost eight times more likely if they appeared to be Arab.\textsuperscript{128} A former French ombudsman has said that “compared to the general population and all other things being equal, young men in France, who are perceived as Arab/Maghrebin or Black, are 20 times more likely to be subjected to identity checks than others”.\textsuperscript{129} The UN High Commissioner for Human Rights singled out France in relation to discriminatory police stops in June 2021.\textsuperscript{130}

The following month, six civil society organisations filed a class action lawsuit demanding structural reforms and measures to end discrimination in police practices, including tighter regulation, improved police training and reporting around identity checks and their impact.\textsuperscript{131} Previously, in a 2016 case, the Court of Cassation recognised state responsibility for a case involving discriminatory identity checks of three people, treatment that amounted to “gross misconduct”.\textsuperscript{132} The court underlined the fact that checks were undertaken for one and a half hours, targeted members of “visible minorities”, and the state failed to show that there were objective reasons to justify the checks.

In Italy, ethnographic studies indicate similar problems. The academic Martina Tazzioli has undertaken extensive fieldwork in the border region between Italy and France – an internal border between two EU member states at which there is now a push to increase identity checks (an issue explained further below). When the Arab Spring uprisings resulted in a spike in irregular departures of people across the Mediterranean, Tazzioli found that:


disparities to promote best practices for police in the realm of non-discrimination.\textsuperscript{124} Under this pilot, “stop forms” were adopted. Records of stops across five Spanish police departments demonstrated that the act of recording stop and search activities led to fewer discriminatory checks.\textsuperscript{125} However, the national police body has shown little interest in following suit.\textsuperscript{126} In localities where the model has been introduced, lack of feedback from senior officials has contributed to lower rates of improvement, while in Girona, police officers even increased apprehensions of non-white people out of frustration with the new policy.\textsuperscript{127}

In France, as in Spain, there is no official collection of data on the ethnicity of people stopped for identity checks. An Open Society Initiative study conducted in 2009 identified that people were six times more likely to be stopped if they were black, and almost eight times more likely if they appeared to be Arab.\textsuperscript{128} A former French ombudsman has said that “compared to the general population and all other things being equal, young men in France, who are perceived as Arab/Maghrebin or Black, are 20 times more likely to be subjected to identity checks than others”.\textsuperscript{129} The UN High Commissioner for Human Rights singled out France in relation to discriminatory police stops in June 2021.\textsuperscript{130}

The following month, six civil society organisations filed a class action lawsuit demanding structural reforms and measures to end discrimination in police practices, including tighter regulation, improved police training and reporting around identity checks and their impact.\textsuperscript{131} Previously, in a 2016 case, the Court of Cassation recognised state responsibility for a case involving discriminatory identity checks of three people, treatment that amounted to “gross misconduct”.\textsuperscript{132} The court underlined the fact that checks were undertaken for one and a half hours, targeted members of “visible minorities”, and the state failed to show that there were objective reasons to justify the checks.

In Italy, ethnographic studies indicate similar problems. The academic Martina Tazzioli has undertaken extensive fieldwork in the border region between Italy and France – an internal border between two EU member states at which there is now a push to increase identity checks (an issue explained further below). When the Arab Spring uprisings resulted in a spike in irregular departures of people across the Mediterranean, Tazzioli found that:
The possibility of enhanced surveillance and checks at the internal borders of the Schengen area is now likely to be enshrined in law, under proposals published in December 2021. These would permit increased patrols at the EU’s internal borders in order to prevent “secondary movements” – that is, the unauthorised movement of individuals, in particular asylum-seekers and refugees, from one member state to another. The Commission has acknowledged that the new measures could “increase the risk” of racial profiling and discriminatory selection of the persons being checked with the border areas,” but has offered no specific safeguards against this possibility, beyond those that already exist (for example, in the EU Charter of Fundamental Rights).

Research in the UK by the Racial Justice Network, Yorkshire Resists and Queen Mary University has shown “systematic racial bias” in the use of mobile fingerprint scanners for police identity checks. The research, based on data gathered despite these well-documented and long-standing issues with police identity checks, the EU is set to provide new technical and legal means for increasing the frequency with which they are carried out. As noted in section Biometric identification: a European priority, a key aim of the interoperability project is to establish a vast, centralised pool of identity data, through the construction of the Common Identity Repository, to “make it easier for authorised officers to reliably identify third-country nationals who are entering, or who are already on, the territory of the Schengen area.”

While the CIR will provide the technical backbone, the drive to step up identity checks is being reinforced by legal and policy initiatives. In May 2017, the European Commission published a ‘Recommendation on proportionate police checks’. The document said that due to terrorism, cross-border crime and irregular migration:

“...the intensification of police checks in the entire territory of Member States, including in border areas and the carrying-out of police checks along the main transport routes such as motorways and railways, may be considered necessary and justified.”


141 Gisti noted in its examination of jurisprudence that mere reference to the ‘Vigipirate’ security alert system do not suffice to justify identity checks, which are governed by Article 78-2 of the penal procedure code.


from UK police forces covering the period from March 2019 to June 2020, found that:

“For every White North European person stopped and scanned in every 10,000 people, 48 Arabic people are scanned on average across the police jurisdictions. 14 Black residents are scanned for every White North European, 14 Asian people, almost 4 Chinese people or 2 South East Asian people for every White North European.”

The groups recommended that the use of mobile fingerprint scanners “should immediately cease until equality impact assessments have been completed with rigour,” and their use should be closely monitored if they are reintroduced. More fundamentally, the report called on police forces and the Home Office to address institutional racism; for a “fire-wall” between policing and immigration services; and for an end to the UK’s “hostile environment” policies, which the authorities are currently seeking to digitise.

The Greek authorities are seeking to implement a similar programme. Backed by EU funding, the police are acquiring portable facial, fingerprint and vehicle number plate recognition devices that will allow officers to instantly run checks against “data already stored in 20 databases held by national and international authorities.” Following a complaint from the human rights organisation Homo Digitalis, the data protection authority launched an investigation into the legality of the program, but this has not yet concluded. The programme is explicitly designed to increase the number of identity checks, and Human Rights Watch has highlighted that the use of biometric technologies in this context “could exacerbate... abusive police tactics, which constitute racial and other forms of profiling and harassment”.

Unwarranted discrimination is prohibited in both the EU and the Council of Europe, under the EU’s Charter of Fundamental Rights and the European Convention on Human Rights. Nevertheless, it is evident that the reality diverges significantly from what is prescribed on paper. Notwithstanding obligations on the authorities to carry out data protection impact assessments and equality impact assessments, the push to bring these technologies into the street is likely to exacerbate existing problems with racial and ethnic profiling, calling for renewed responses from community groups, civil society organisations and all those seeking a more just society.

149 Ibid.
Mass biometric surveillance in Italy: on hold, for now

The increasing collection and centralisation of biometric data has primarily been criticised for the potential it offers for the introduction of mass surveillance, in particular through the use of facial recognition technology. The Italian authorities have enthusiastically sought to adopt such systems. The SARI (Sistema Automatico Riconoscimento Immagini) system was acquired by the police’s Direzione Centrale Anticrimine in 2017 with money from the EU’s Internal Security Fund.150

SARI Enterprise would be used to check the authenticity of document photos and conduct automatic checks matching facial images with images from the country’s automated fingerprint identification system, which also stores photos. It was authorised by the ombudsman in July 2018 to speed up procedures already undertaken using less efficient means (checking details like eye colour or tattoos) to identify wanted people.

In the same year, plans to use SARI Real-Time as a “tactical system to monitor disembarkation operations and the various types of related illegal activities, filming them and identifying the people involved” were stalled.151 A 2017 tender mentioned “support for territorial control operations during events and/or demonstrations,”152 making clear that these technologies can be used not just to target non-citizens and racialized minorities, but protesters and dissidents as well.

The Italian system was to rely on a network of video-cameras to provide real-time comparison with a watchlist containing up to 10,000 facial images, with alerts issued to police officers in case of a match. The privacy ombudsman did not authorise deployment of SARI Real-Time and in 2021 ruled that the system lacked a legal basis for automatic processing of facial images, and was planned as a form of indiscriminate, mass surveillance.153 The ombudsman drew on Council of Europe guidelines to highlight the sensitivity of this matter, noting that the deployment of SARI Real Time would amount to large-scale automated processing of data that may affect participants in social and political demonstrations who are not subject to police “attention”.

The case of SARI Real Time has been highlighted by campaigners calling for a ban on biometric mass surveillance in the EU. The current stage for this struggle is the proposed Artificial Intelligence Act, which in its current form prohibits “real-time biometric identification” in public spaces in principle, but in practice provides multiple carve-outs for law enforcement authorities to deploy such systems.

The campaign Reclaim Your Face is calling for an outright ban, in order to prevent the unwarranted tracking, categorisation and monitoring of individuals. The campaign warns that this form of surveillance “threatens everyone’s rights and freedoms to participate in public and political life.” However, it must be noted that given the amount of biometric data stored by EU states on foreign nationals, it is likely to disproportionately affect non-citizens. For example, in the case of SARI Real Time, the database underpinning the system contains data on two million Italian citizens, and seven million foreigners.154
6.
Conclusion
The biometric registration of all foreign nationals present in the EU is a long-standing EU policy objective, and one that is coming increasingly close to being achieved. While many would argue that this is unproblematic provided that the necessary privacy and data protection safeguards are applied and adhered to, this view ignores two issues. Firstly, such systems are designed to make it easier to exclude certain categories of people from EU territory and participation in society, raising the need to question their premises and the laws and policies that underpin them. Secondly, like any other technology, these systems are introduced into a particular social context that will shape the ways in which they are used.

As this report has argued, the introduction of new technologies to increase the number of identity checks by police and immigration authorities is likely to see ethnic minority citizens and non-citizens subjected to a growing number of unwarranted intrusions into their everyday activities, given the treatment of skin colour as a proxy for immigration status. In particular, the existence of a huge database holding data solely on foreign nationals and explicit policy instructions to step up identity checks means that the introduction of the Common Identity Repository and the mobile biometric technology required to access it is likely to exacerbate the racist policing and ethnic profiling that already exist across the EU.

The growing number of initiatives that seek to make connections between anti-racist campaigns, migrants’ rights organisations, privacy and data protection advocates and technology specialists will play an important role in challenging these developments in the years to come. The broader social concern with issues of racism and racial equality that has been propelled by the global eruption of anti-racist protests in response to the killing of George Floyd by a police officer in the USA in June 2020, and the broader societal fascination with new technologies, may provide fertile ground for these initiatives to expand. At the same time, it is crucial that a focus on technology itself does not draw attention away from the structures lying behind it: new technologies may increase the capacity for harm, but are not necessarily the underlying driving force.

It must be recognised that the broader political climate of xenophobia and nationalism is not particularly favourable to these efforts. Attempts to prevent the use of new technologies from entrenching racist and discriminatory practices will need to work on a variety of fronts: know your rights campaigns and community organising; administrative and legal complaints to uphold privacy and data protection rights; demands for adequate funding and resources for the data protection authorities responsible for overseeing the work of the police and immigration authorities, and for ‘firewalls’ between policing and public services; critical research and investigative journalism to inform campaigns and complaints; calls for public funds not to be used in research likely to help entrench discrimination; and efforts to ensure transparency in law, policy-making and enforcement. All of these are vital for ensuring that state authorities are held politically and publicly accountable, and for developing more equal and just alternatives.

Authors
Chris Jones, Jane Kilpatrick, Yasha Maccanico

Acknowledgements
The authors wish to thank all those who gave their time to be interviewed as part of the research for this report, and all those who participated in the workshops hosted by Statewatch on the issue of biometric identification technologies and racism and discrimination in October 2021.

Methodology
This report is based on desk research into open and closed sources, individual interviews, and the insights generated during the workshops noted above. It was produced as part of the project ‘Protecting migrant communities by future-proofing the immigration data system’, supported by Privacy International.

About Statewatch
Statewatch produces and promotes critical research, policy analysis and investigative journalism to inform debates, movements and campaigns on civil liberties, human rights and democratic standards. We began operating in 1991 and are based in London.

Published by Statewatch, February 2022