AUTOMATED SUSPICION

THE EU'S NEW TRAVEL SURVEILLANCE INITIATIVES

statewatch

Author: Chris Jones

Additional research: Yurema Pallarés Pla

Thanks to Tony Bunyan, Sean Burke, Yasha Maccanico, Antonella Napolitano, Alyna Smith and Frances Webber.

This report was produced as part of the project 'Biometric Europe: imposing digital identities in the name of security'.

Published by Statewatch, July 2020.

Statewatch is the operating name of the Libertarian Research & Education Trust. UK charity number: 1154784, UK company number: 08480724.

CONTENTS

List of abbreviations/acronyms

CIR	Common Identity Repository
ECRIS-TCN	European Criminal Records Information System for Third-Country Nationals
EES	Entry/Exit System
ETIAS	European Travel Information and Authorisation System
EU	European Union
Europol	European Agency for Law Enforcement Cooperation
Frontex	European Border and Coast Guard Agency
Interpol	International Criminal Police Organization
MID	Multiple Identity Detector
PNR	Passenger Name Record
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents
TDAWN	Travel Documents Associated With Notices
VIS	Visa Information System

EXECUTIVE SUMMARY

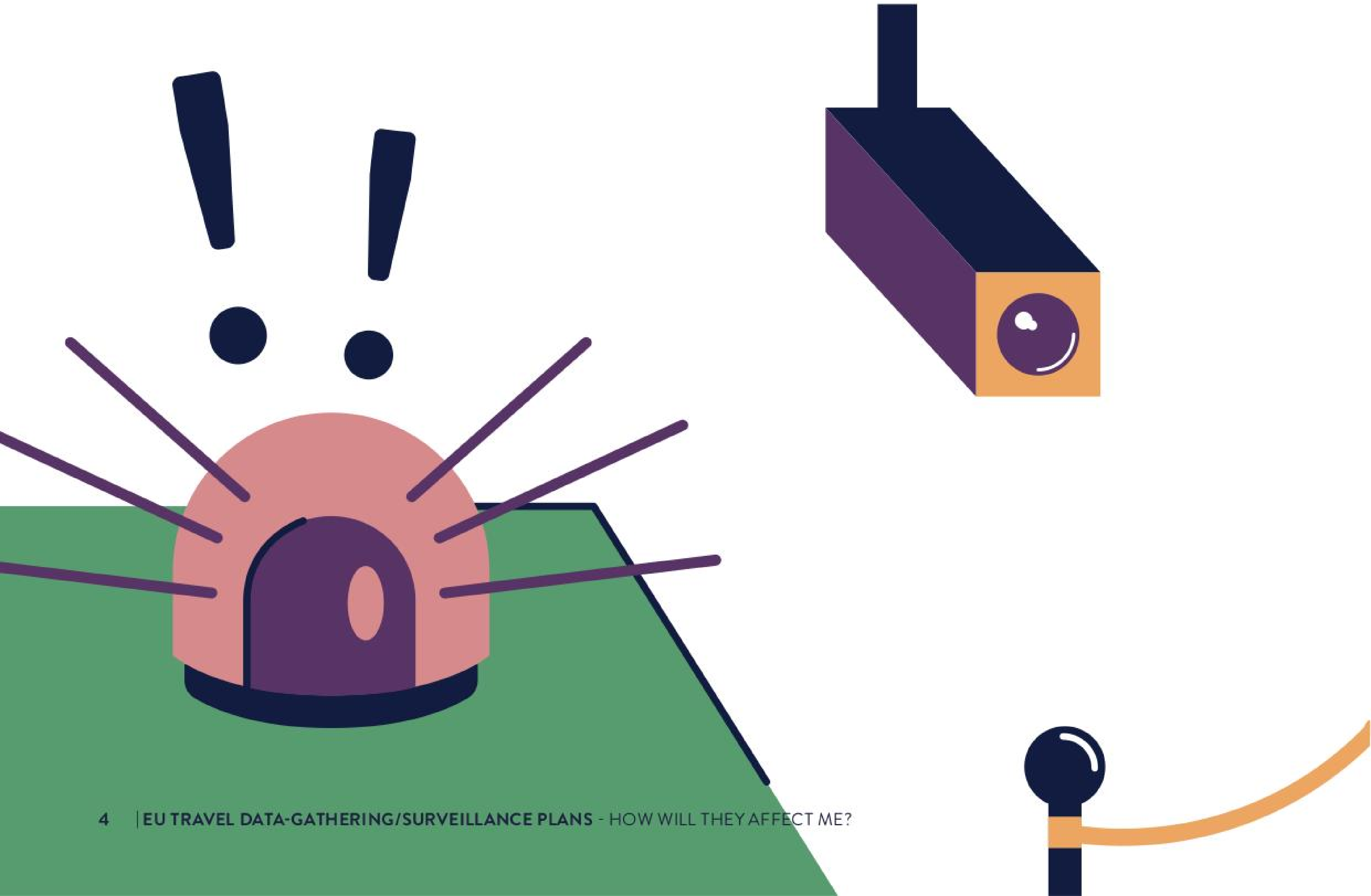
The ongoing coronavirus pandemic has raised the possibility of widespread surveillance and location tracking for the purpose of disease control, setting alarm bells ringing amongst privacy advocates and civil rights campaigners. However, EU institutions and governments have long been set on the path of more intensive personal data processing for the purpose of migration control, and these developments have in some cases passed almost entirely under the radar of the press and civil society organisations.

This report examines, explains and critiques a number of large-scale EU information systems currently being planned or built that will significantly extend the collection and use of biometric and biographic data taken from visitors to the Schengen area, made up of 26 EU member states as well as Iceland, Liechtenstein, Norway and Switzerland. In particular, it examines new systems being introduced to track, analyse and assess the potential security, immigration or public health risks posed by non-EU citizens who have to apply for either a short-stay visa or a travel authorisation – primarily the Visa Information System (VIS), which is being upgraded, and the European Travel Information and Authorisation System (ETIAS), which is currently under construction.

The visa obligation has existed for years. The forthcoming travel authorisation obligation, which will cover citizens of non-EU states who do not require a visa, is new and will massively expand the amount of data the EU holds on non-citizens. It is the EU's equivalent of the USA's ESTA, Canada's eTA and Australia's ETA.[1] These schemes represent a form of "government permission to travel," to borrow the words of Edward Hasbrouck,[2] and they rely on the extensive processing of personal data.

Data will be gathered on travellers themselves as well as their families, education, occupation and criminal convictions. Fingerprints and photographs will be taken from all travellers, including from millions of children from the age of six onwards. This data will not just be used to assess an individual's application, but to feed data mining and profiling algorithms. It will be stored in large-scale databases accessible to hundreds of thousands of individuals working for hundreds of different public authorities.

Much of this data will also be used to feed an enormous new database holding the 'identity data' – fingerprints, photographs, names, nationalities and travel document data – of non-EU citizens. This system, the Common Identity Repository (CIR), is being introduced as part of the EU's complex 'interoperability' initiative and aims to facilitate an increase in police identity checks within the EU. It will only hold the data of non-EU citizens and, with only weak anti-discrimination safeguards in the legislation, raises the risk of further entrenching racial profiling in police work.



The remote monitoring and control of travellers is also being extended through the VIS upgrade and the introduction of ETIAS. Travel companies are already obliged to check, prior to an individual boarding a plane, coach or train, whether they have the visa required to enter the Schengen area. This obligation will be extended to include travel authorisations, with travel companies able to use the central databases of the VIS and ETIAS to verify whether a person's paperwork is in order or not. When people arrive at the Schengen border, when they are within the Schengen area and long after they leave, their personal data will remain stored in these systems and be available for a multitude of further uses.

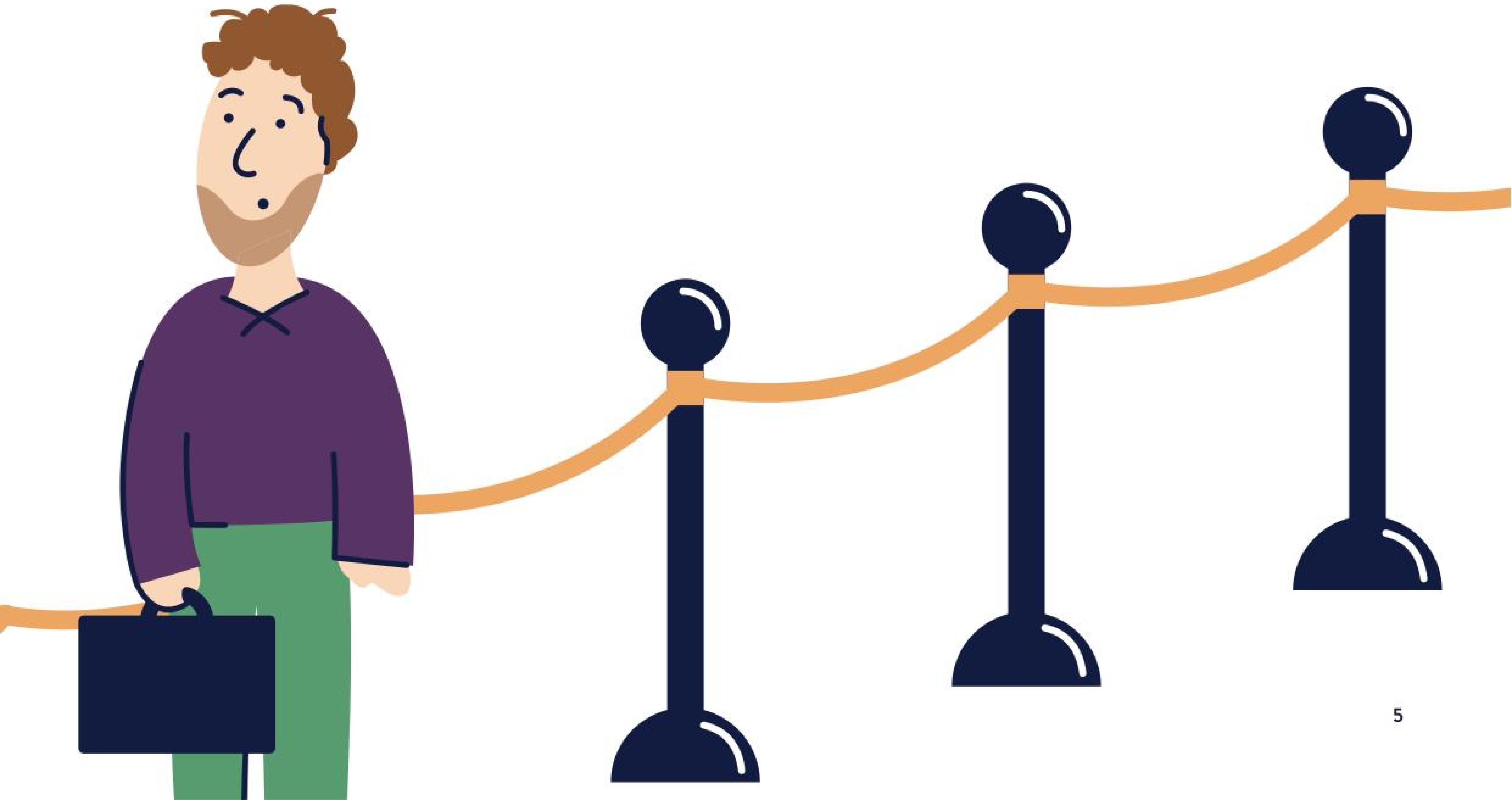
These new systems and tools have been presented by EU institutions as necessary to keep EU citizens safe. However, the idea that more personal data gathering will automatically lead to greater security is a highly questionable claim, given that the authorities already have problems dealing with the data they hold now.

Furthermore, a key part of the 'interoperability' agenda is the cross-matching and combination of data on tens of millions of people from a host of different databases. Given that the EU's databases are already-known to be strewn with errors, this massively increases the risks of mistakes in decision making in a policy field – immigration – that already involves a high degree of discretion and which has profound implications for peoples' lives.

These new systems have been presented by their proponents as almost-inevitable technological developments. This is a misleading idea which masks the political and ethical judgments that lie behind the introduction of any new technology. It would be fairer to say that EU lawmakers have chosen to introduce unproven, experimental technologies – in particular, automated profiling – for use on non-EU citizens, who have no choice in the matter and are likely to face difficulties in exercising their rights.

Finally, the introduction of new databases designed to hold data on tens of millions of non-citizens rests on the idea that our public authorities can be trusted to comply with the rules and will not abuse the new troves of data to which they are being given access. Granting access to more data to more people inevitably increases the risk of individual abuses. Furthermore, the last decade has seen numerous states across the EU turn their back on fundamental rights and democratic standards, with migrants frequently used as scapegoats for society's ills. In a climate of increased xenophobia and social hostility to foreigners, it is extremely dangerous to assert that intrusive data-gathering will counterbalance a supposed threat posed by non-citizens.

Almost all the legislation governing these systems has now been put in place. What remains is for them to be upgraded or constructed and put into use. Close attention should be paid by lawmakers, journalists, civil society organisations and others to see exactly how this is done. If all non-citizens are to be treated as potential risks and assessed, analysed, monitored and tracked accordingly, it may not be long before citizens come under the same veil of suspicion.



INTRODUCTION

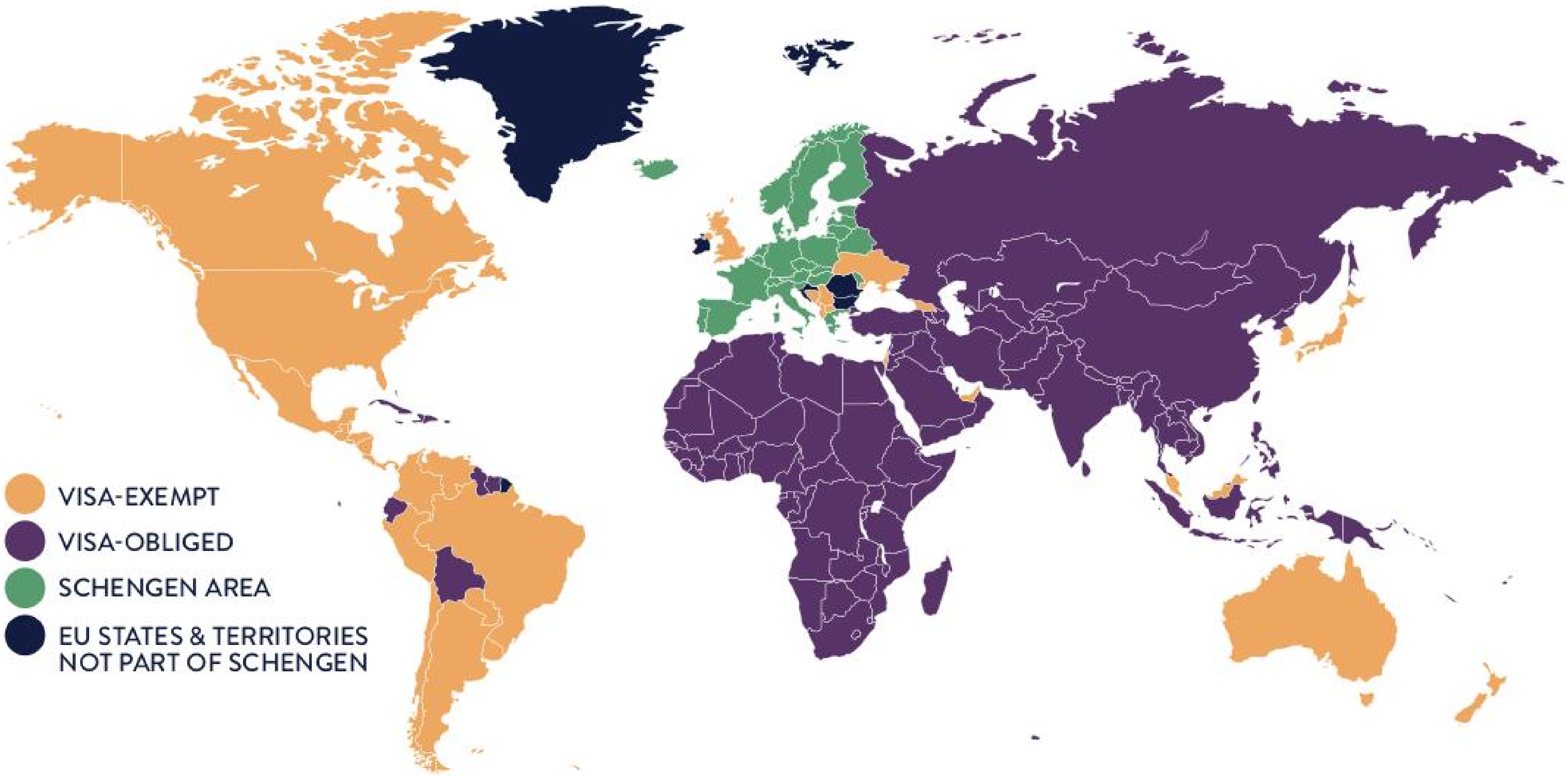


Figure 1: Visa requirements for the Schengen area.

SOURCE: EUROPEAN COMMISSION

Until the arrival of the novel coronavirus pandemic in early 2020, it was a widely-held assumption amongst many people that international travel had never been so fast or simple. The pandemic has changed that, at least for the time being. However, even before the imposition of lockdowns and quarantines across the world, the reality was somewhat different, depending on who you are and where you are from.

Some five billion citizens of 105 countries around the world must acquire a visa if they wish to enter the Schengen area (made up of 26 of the EU's member states along with Iceland, Liechtenstein, Norway and Switzerland). These 105 states are generally amongst the world's poorest and often suffer from violent conflict, repression, and serious economic, social and political problems. Meanwhile, there are some 1.4 billion citizens of around 60 countries who do not require a visa, but who will soon be required to apply for a "travel authorisation". This is intended to serve the same purpose: an assessment of whether or not an individual is a 'bona fide' traveller (in the original version of the map above, the European Commission uses red for visa-obliged states, a fairly blunt way of representing the supposed risk posed by their citizens). Travel authorisations and short-stay visas[3] allow the holder to spend 90 days within any 180-day period within the Schengen area.

Applying for a visa is already an intrusive process, but in the coming years applicants for both visas and travel authorisations will be obliged to reveal increasing amounts of sensitive personal information to EU authorities. Through the introduction of new technologies – 'interoperable' databases, automated profiling algorithms and data mining tools – along with 'pre-crime' watchlists for potential criminals and terrorists, their data will be processed in a range of new ways and made available to a wide variety of authorities across the EU and beyond.[4]

This report provides a critical examination of forthcoming EU initiatives that will deploy these technologies for the intensified processing of personal data. It seeks to inform civil society – NGOs, campaigners, journalists, researchers and anyone with an interest in the topic – how these processes will work and the implications for fundamental rights, with the aim of spurring further investigation and action.

The introduction of new systems for the increased processing of personal data on visitors to the EU is indicative of broader trends towards the more intensive collection and examination of personal data by both public institutions and private companies. While this is facilitated by new technological capabilities, it is primarily the result of a deliberate intermingling of security and migration policies, a process which has been ramped up in the last five years as EU institutions and national governments attempt to assert their legitimacy and authority by casting migrants as objects of suspicion; potential threats who require close monitoring and supervision lest they try to undermine "our European way of life"[5] in one way or another.

The report is structured on the basis of a journey an individual, and their personal data, would take if they wished to travel to the Schengen area. The first step is making an application for a visa or travel authorisation and what happens to the personal data that must be provided. This is the longest section of the report, due to the range of new procedures that are being introduced – automated checks against other databases, a new profiling system and checks against a pre-crime 'watchlist', amongst other things. The second step is the journey itself, whether by plane, train, boat, coach or some other means. The third step in the journey is arrival at the border. The fourth step is the time an individual spends within the Schengen area. The fifth and final step is an individual's departure and what happens to their data when they leave. Along the course of this journey, some of the processes to which the two groups of travellers will be subjected are the same, and so they are examined together. Elsewhere, they are looked at separately.

Much of the law governing the systems examined in this report is already in place, leaving little room for legislative lobbying. However, this does not mean there is nothing left to be done to challenge the dangers these systems pose for fundamental rights. Some implementing legislation still has to be agreed and, as highlighted in this report, existing national and EU systems that use similar technologies and practices are the subject of ongoing court cases. There is much that campaigners, civil society organisations, journalists and others can do to limit or even remove the veil of suspicion being placed over visitors to the Schengen area.

STEP ONE:

MAKING AN APPLICATION

VISAS

Visa applications are generally submitted on paper at the embassy or consulate of a Schengen state. Applicants must hand over significant amounts of personal data to the authorities including, amongst other things, information on their identity, employment, education and, if applicable, the personal details of the person or organisation inviting them to the Schengen area.

Biometrics are a key part of the EU's visa regime, with ten fingerprints and a photograph taken from every applicant aged 12 or over. Legal proposals currently under discussion would lower the minimum age to six. This would mean the storage of biometric data from up to a million more children in the central database of the EU's Visa Information System (VIS), which at the end of 2018 held 42 million fingerprint sets in total. A recent upgrade expanded the database so that it can hold a total of up to 100 million visa applications.[6]

Applicants also have to demonstrate that they have valid medical insurance for their trip and visa authorities are able to request extensive further documentation, if so desired. This might include bank statements, travel tickets, proof of accommodation, employment, property ownership, or even "proof of integration in the country of residence," amongst other things. Applicants may also be called to attend an interview, so that officials can better assess their trustworthiness.

If an application is admissible – that is, the form is complete, biometrics have been taken and the fee paid – a file is created in the VIS. This contains a sub-set of the data in the application form, including names; sex; date, place and country of birth; travel document details; and purpose of travel. Application files can be linked to one another (for example, those of family members or previous applications), offering something of an investigative function to officials, who are able to see with whom an individual has familial, social or professional ties.

Data held in the system is accessible by hundreds of thousands of officials working for hundreds of EU and national authorities. By September 2017, "the approximate total number of end-users accessing VIS" for purposes related to visa applications, identity checks and asylum applications was "more than 458,000,"[7] with 116 national authorities granted access as of May 2016 (the most recent figures available).[8] For the purposes of law enforcement access to the VIS (see 'Step five: Departure'), at the end of September 2017 there were 3,867 "access points" and 7,343 user accounts.[9]

It is likely that in the future the entire application process will be digitised, allowing all visa application data to be entered into the system. This will facilitate "behind-the-scenes risk analysis" and "data-driven algorithms that translate the common visa policy into checks and alerts," according to a study carried out for the European Commission.[10]

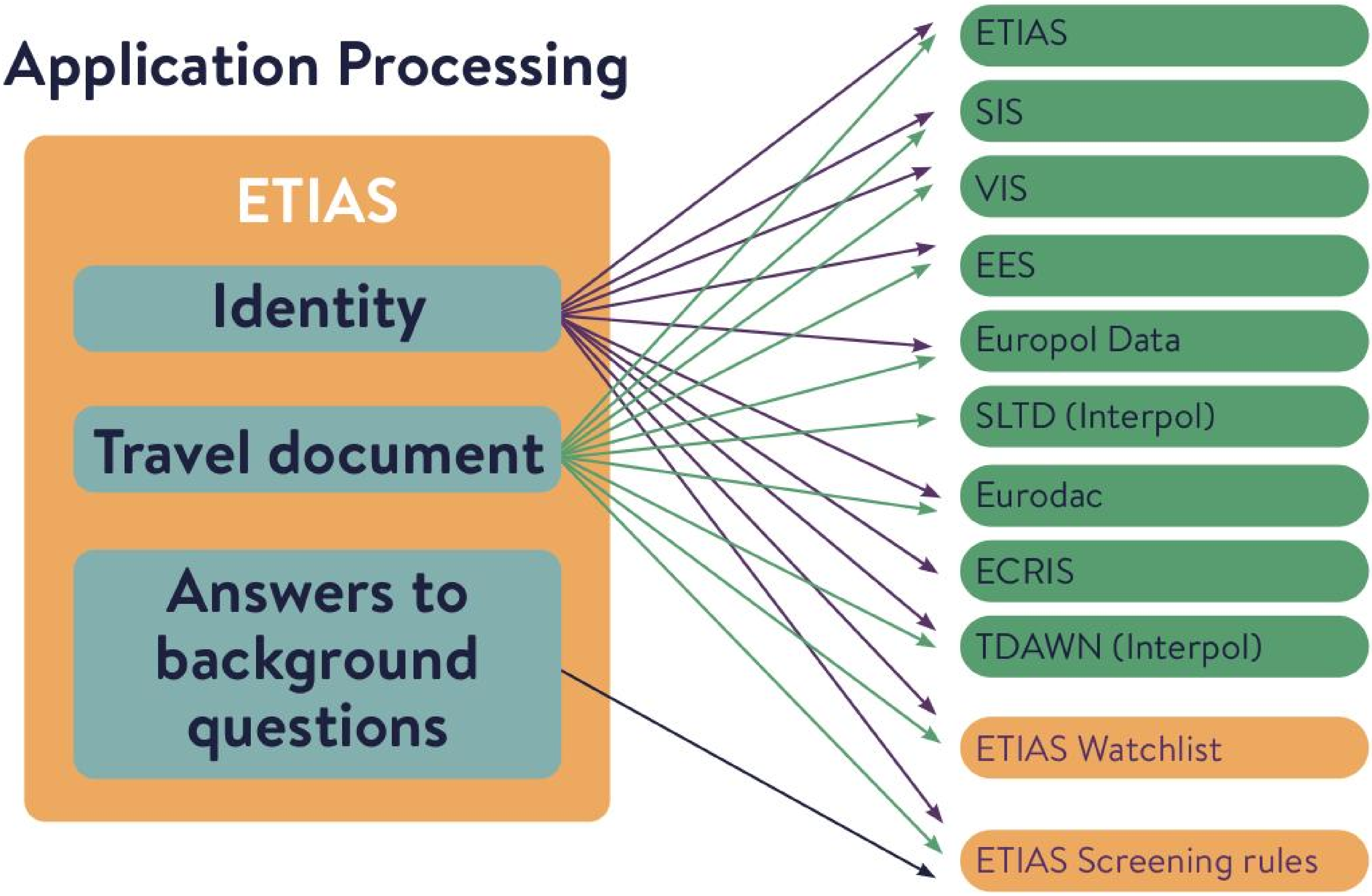
TRAVEL AUTHORISATIONS

Citizens of visa-exempt countries will have to provide a significant amount of personal data as part of their travel authorisation application, which will be submitted through an online portal and stored in a new database, the European Travel Information and Authorisation System (ETIAS). Amongst other things, the data required for a travel authorisation will include names, address, age, nationality, occupation, level of education and the names of the applicant's parents.

Biometrics will not be stored in the ETIAS. However, anyone granted a travel authorisation will have four fingerprints and a photograph taken when they arrive at the Schengen border, for inclusion in the Entry/Exit System (EES), another new database that will record border crossings and provide national authorities in the EU with lists of 'overstayers' – those who stay longer than permitted in the Schengen area – with the aim of aiding in their detection and expulsion. The EES is expected to hold files on almost 50 million visa-exempt travellers by 2025.

Travel authorisation applicants will also be asked to answer questions on whether they have been convicted of criminal or terrorist offences, whether they have been present in a conflict or war zone (and if so, why) and whether they have ever been subject to a deportation order. The authorities may also request additional documentation or information from applicants, who can be called to an interview if deemed necessary. As with an interview for a visa, the purpose would be to better assess the trustworthiness of the individual.

If an application is admissible – that is, the form is complete and the fee (€7) has been paid – a file is automatically created in the ETIAS Central System. These contain a reference number, the status of the application, the date and time of submission and all the data submitted in the application form. As with the VIS, new application files can be linked to previous ones, offering something of an investigative function to officials. Given that the ETIAS is not yet up and running, it is unknown how many authorities or individuals have access, but the numbers are likely to be extremely high.



How data from travel authorisation applications will be checked against EU and Interpol databases. Similar rules will be put into effect for the visa application data held in the VIS.

SOURCE: EUROPEAN COMMISSION

Feeding the EU’s new identity database

In the coming years, data from both visa applications and travel authorisations will be used as a source of data for another new EU database currently under construction, called the Common Identity Repository (CIR). Identity data collected from visa and travel authorisation holders – names, date and place of birth, sex, travel document data, fingerprints and a photograph – will be stored in the CIR, while other data relating to the visa or travel authorisation application – for example, the purpose of travel or the applicant’s occupation – will remain in the VIS and ETIAS.

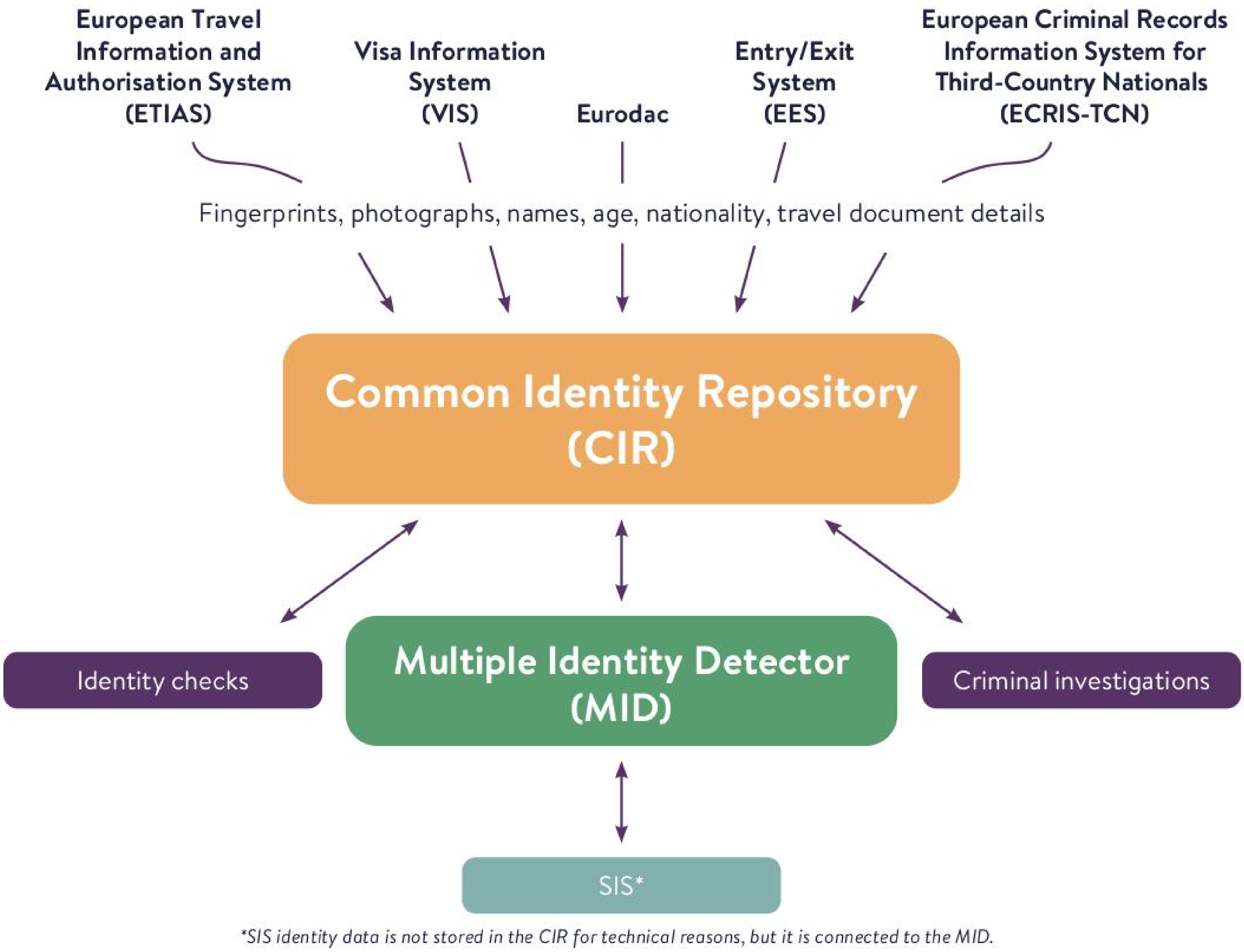
The same process will be applied to three other large-scale EU databases: the Entry/Exit System (EES), which will record all border crossings in and out of the Schengen area; Eurodac, which stores data on all asylum-seekers in the EU and is being expanded to also hold information on undocumented migrants; and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN), which will hold data on non-EU citizens convicted in one or more EU member state. The CIR will initially be able to hold up to 300 million individual records.

Once in the CIR, this data will be used for purposes beyond those of the underlying databases. While data from the VIS and ETIAS is primarily gathered for processing visa and travel authorisation applications, the transfer of ‘identity data’ to the CIR will be used to facilitate identity checks by police officers and other officials, assist in law enforcement investigations, and even help with the gruesome task of identifying dead people. It will also be used for new, automated procedures that will try to detect the use of false identities by non-EU nationals, through the large-scale comparison of biometric and biographic data across the different systems. In the words of one critic, this equates to pulling “a new legal basis out of a hat, after you have already collected personal data.”[11]

The interoperability plan is controversial for a number of reasons. By breaking the ‘silo’ model of data management in the EU, whereby personal data was held in separate databases for strictly defined purposes, it breaches one of the basic principles of data protection law, known as purpose limitation. According to this rule, personal data should be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.”[12] As the European Commission remarked in 2010: “A single, overarching EU information system with multiple purposes would deliver the highest degree of information sharing,” but would also be “a gross and illegitimate restriction of individuals’ right to privacy and data protection”.[13] Clearly, times have changed.

The legislation on identity checks also fails to meet EU legal standards on police access to personal data due to weak anti-discrimination safeguards, no evidence that non-EU nationals are more likely to pose a security threat than EU nationals (whose data is not stored in any similar type of database) and a failure to clearly define the specific offences or legal thresholds that could justify access to the database.[14]

The merging and comparison of so much personal data from so many different systems also raises issues regarding the ability of data subjects to know who has access to their data, what is being done with it, and how they can correct it should it be erroneous. It may be particularly difficult for non-EU citizens to exercise their data rights due to language barriers and legal complexity.[15]


European Travel Information and Authorisation System (ETIAS)
Visa Information System (VIS)
Eurodac
Entry/Exit System (EES)
European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)
Fingerprints, photographs, names, age, nationality, travel document details
Common Identity Repository (CIR)
Identity checks
Multiple Identity Detector (MID)
Criminal investigations
SIS*
*SIS identity data is not stored in the CIR for technical reasons, but it is connected to the MID.

How the new Common Identity Repository and Multiple Identity Detector will function

Source	VIS	ETIAS	EES			
			Visa-obliged		Visa-exempt	
Data type			Entry	Refusal	Entry	Refusal
Biometric data						
Fingerprints (number of prints)	X (ten)			X* (four)	X (four)	X* (four)
Facial image	X		X	X*	X	X*
Biographic data						
First name(s)	X	X	X	X	X	X
Surname	X	X	X	X	X	X
Former surname(s)	X					
Name at birth		X				
Previous names						
Previously used names						
Aliases, pseudonyms, artistic names, usual names		X				
Parents' first names		X				
Date of birth	X	X	X	X	X	X
Place of birth	X	X				
Nationality(ies)		X	X	X	X	X
Sex	X	X	X		X	X
Gender						
Travel document data						
Type and number	X	X	X		X	X
Issuing country code	X	X	X		X	X
Validity	X	X	X		X	X
Application data						
	Application number and status	Application number and status	Date, time and border crossing point of entry	Date, time and border crossing point of refusal	Date, time and border crossing point of entry	Date, time and border crossing point of refusal
	Authority responsible for visa application / issuance / refusal	Date and time of application submission	Visa data, i.e. number and authorised stay	Reasons for refusal of entry	Exit data	Reasons for refusal of entry
	Place and date of application	IP address	Date, time and border crossing point of exit		Date, time and border crossing point of exit	
	Type of visa and validity period (if issued)		Remaining authorised stay		Remaining authorised stay	
	Details of the person/company inviting and/or liable to pay applicant's subsistence costs Main destination and duration of stay	Data of the person/company making the application, if not the traveller Member state of first intended stay and (optional) address of first intended stay				
	Purpose of travel					

Data storage in the EES, ETIAS, VIS and CIR (grey cells = data held in the CIR)

	Date of arrival and departure					
	Border of first entry					
	Residence	Home address and/or city and country of residence, email address and phone number(s)				
	Current occupation and employer; for students, name of school	Occupation and level of education				
	For minors, parents' names	For minors, names, address, email address and phone number(s) of parental authority or guardian				
	Scan of biographic data page of the travel document					
		If claiming status as family member of an EU citizen, their familial ties and details of the family member				
		Criminal convictions in last 10 or 20 (in case of terrorism) years				
		Stay in conflict or war zone in last 10 years				
		Subject to a deportation order in last 10 years				
	Results of the automated processing against databases, information systems and the watchlist	Results of the automated processing against databases, information systems and the watchlist				
		Any 'flag' added to the application				
Retention period						
	Five years	Three years (with optional three year renewal, subject to traveller's consent)	Three years	Five years	Three years	Five years

Data storage in the EES, ETIAS, VIS and CIR (grey cells = data held in the CIR)

*If the person is refused entry because of a false / counterfeit / forged travel document, visa or residence permit; or because they are subject to SIS or national alert on refusal of entry.

PROCESSING APPLICATIONS: NEW AUTOMATED CHECKS

VISAS

The processing of visa applications is at present largely done manually, with officials making checks against two databases: the VIS, to see whether any previous applications by the same individual exist; and in the Schengen Information System (SIS, a vast EU database for police, judicial and border control cooperation), to see whether they are wanted by the police or subject to an entry ban.[16]

Proposed changes to the visa process would automate most of this work, whilst increasing the number of databases against which applicants are screened. The legislation is currently under negotiation between the European Parliament and the Council of the EU, but when it comes into force the VIS will automatically check other EU and international databases to see if an applicant is wanted by the police, subject to a deportation order or entry ban, has previously applied for asylum in the EU, been apprehended for irregularly crossing an external EU border or being within the EU in an irregular situation, or has been convicted of terrorism or serious criminal offences in the EU.[17]

There will also be automated checks to see if the person has previously applied for a visa; if they have visited the Schengen area in the past and if so, how long for; or if they are listed in any of Europol's databases. A new Multiple-Identity Detector that is being introduced as part of the interoperability agenda will check if their identity data matches that held in any other EU database and, if so, whether they may be using a false identity.[18]

Currently, visa applications are not routinely checked against these databases and the proposal to do so raised some eyebrows amongst data protection specialists, but no serious critiques were forthcoming.[19] However, such checks were already written into law for travel authorisations, and they also apply to EU citizens when they cross the external borders of the Schengen area – in this context, extending the veil of suspicion to visa applicants was a logical step.

'Hits' resulting from these automated checks will have to be manually verified by the visa authorities. If the hits are accurate, and do concern the visa applicant, they must be taken into account in the assessment of the application.[20] Furthermore, the Council of the EU would like to give Europol the power to issue a "reasoned opinion" on applicants whose details trigger a hit in the agency's databases. While not formally binding on the visa authorities, this would be a significant extension of the agency's powers.

TRAVEL AUTHORISATIONS

The ETIAS is intended to be largely automated unless a check against a database, watchlist or profiling system results in a 'hit', at which point an application will be manually processed by national authorities.

Travel authorisation applications will be checked automatically against a host of other EU and international databases. These will see whether the applicant should be refused entry into the Schengen area; is wanted for arrest or extradition; is using a travel document reported as lost or stolen; has previously visited the Schengen area and, if so, how long for; or has ever made a visa application and the results of that application.[21]

Automated checks will also see whether the applicant has previously applied for asylum; been apprehended whilst irregularly crossing an external border or in an irregular situation within the EU; has been convicted of terrorism or other serious criminal offences in the EU; or is listed in any of Europol's databases. A new 'Multiple-Identity Detector' being introduced as part of the interoperability agenda will check if their identity data matches that held in any other EU database and, if so, whether they may be using a false identity.[22]

If these checks lead to hits, the ETIAS Central Unit – which will be operated by Frontex, the EU border control agency – will be given access to the application file and any files linked to it, for verification purposes. National authorities must be consulted on hits against data they have supplied to EU databases and may veto the application if they wish. The same applies to Europol, the EU's policing agency, although it does not have a veto power.[23]

A travel authorisation application must be refused if the applicant is subject to an alert concerning a lost, stolen, misappropriated or invalidated travel document or an alert on refusal of entry or stay. In other cases, the national authorities must use the information available to assess the application.

International document databases as a tool of political persecution

The requirement to check visa and travel authorisation applications against databases of travel documents reported as lost or stolen may, at first glance, appear sensible. However, the main international system for making such reports – Interpol's Stolen and Lost Travel Documents (SLTD) database – is known to have been used by states seeking to persecute their political opponents. In this regard, the automatic refusal of travel authorisations in cases where the document associated with the application is reported as lost or stolen is particularly concerning.

It is well-established that states have used the SLTD database, along with other Interpol mechanisms such as red notices and blue notices,[24] to harass and persecute political opponents.[25] In 2017 the Stockholm Center for Freedom, a human rights organisation started by Turkish exiles in Sweden, documented a number of cases of such persecution by the Turkish state. For example, the journalist Sevgi Akarçesme was removed from a July 2017 flight from Brussels to New York just prior to departure, after the Turkish authorities issued a false notification in the SLTD database. Enes Kanter, a professional basketball player in the USA, narrowly avoided arrest in Indonesia at the Turkish government's behest, only to be detained at an airport in Romania due to a false report in the SLTD database.[26]

Applicants who are refused a visa or travel authorisation have the right to appeal the decision. However, that appeal will be conducted according to the national law of the member state that refused the application, meaning that individuals' rights will differ from state to state. Furthermore, while they must be provided with information on the right of appeal in their native language, applicants who do make an appeal will be left to navigate a foreign legal system in a language in which they are unlikely to be fluent. In any case, who are the authorities more likely to believe – an Interpol notice, or a lone individual?

False identities, or false positives? New technologies in the application procedure

As noted above, one of the new automated checks being introduced into the visa and travel authorisation application procedure concerns the possible use of false identities. As part of the EU's rules on 'interoperability', a new system called the Multiple Identity Detector (MID) will be introduced, with the aim of doing exactly as its name suggests.

When the MID comes into use, every time a file is created in any EU policing or migration database – in this case, the VIS or the ETIAS – the biographic and biometric data it contains will be compared to other EU systems dealing with policing, border control, border crossings, travel authorisations, asylum applications and criminal records. In the event of one or more 'hits' – that is, where data in the new file matches pre-existing data in one or more systems – a file will be created in the MID, containing a 'yellow link' between the two sets of matching data.

The authority that created the file will then have to assess whether the matching sets of data legitimately refer to the same person (e.g. people who have changed their name), illegitimately refer to the same person (i.e. a case of identity fraud), or refer to different people with similar identities, and mark the linked data as such.

Clearly, if a large number of yellow links are generated by the MID in relation to visa applications, the workload of the visa authorities would significantly increase.[27] The same can be said of 'hits' against any other databases following automated checks. The process for clarifying and interpreting those links is to be set out in implementing legislation, which is currently under discussion.[28] That decision may also address whether it should be mandatory to interview individuals whose data gives rise to a yellow link, but its content has not yet been made public.

Quality control

Data quality is another crucial issue for the proper functioning of any database, and is fundamental if the EU's interoperability project is to work as intended. However, the quality of the data stored in the underlying databases that will feed the new 'interoperable' systems is far from perfect, something of which the EU's governments are well aware. In April 2020, a year after the interoperability legislation was adopted, the Council Presidency circulated a paper calling for a "roadmap for standardisation for data quality purposes."[29]

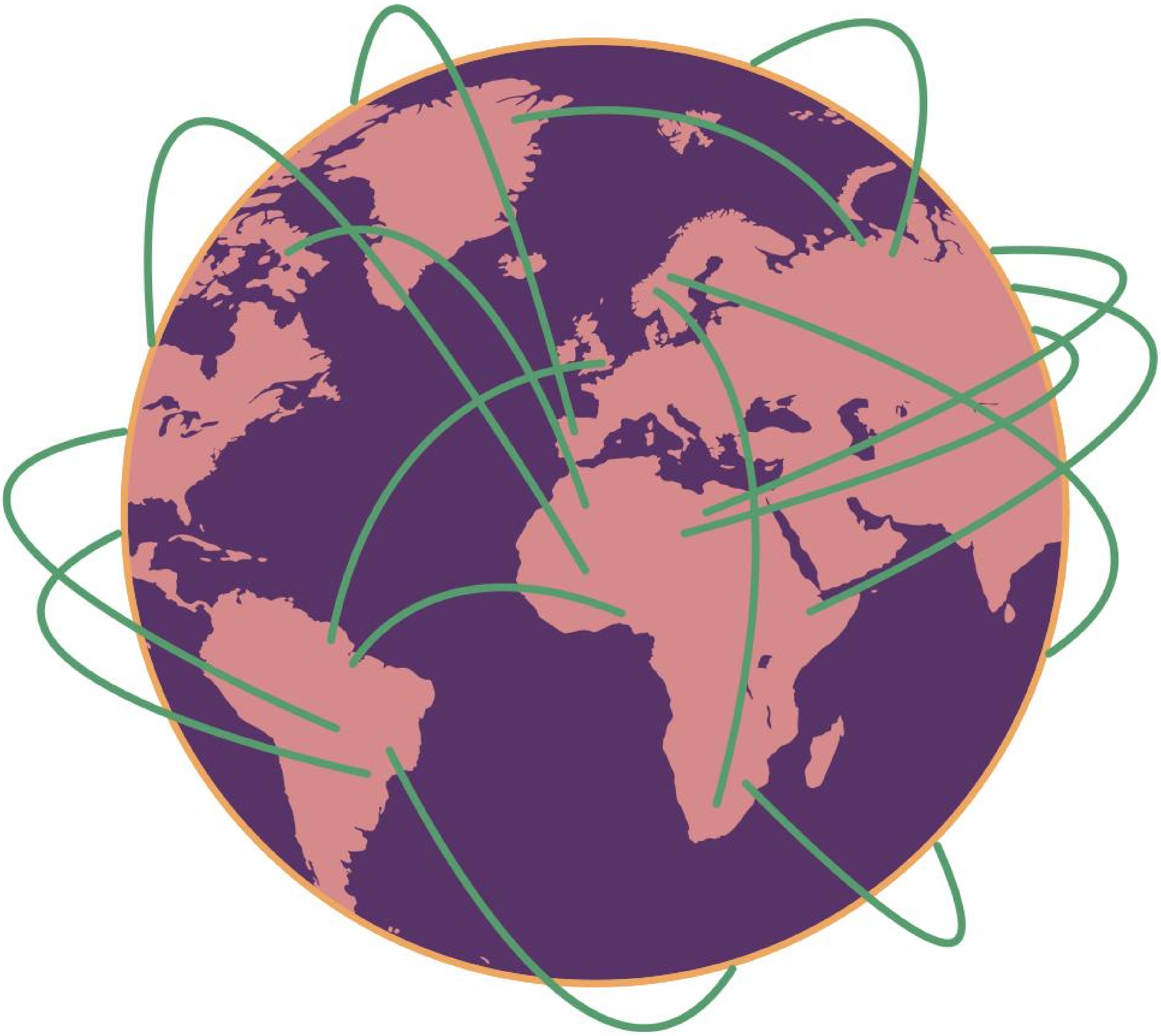
A 2018 study by the EU's Fundamental Rights Agency found data quality problems with all existing large-scale EU databases. With regard to the VIS, the study highlighted cases where biometrics were attached to the wrong application file, resulting in false matches, as well as "significant amounts" of inaccurate data being stored in files.[30] The European Court of Auditors has also highlighted serious issues with data quality in the VIS, as well as the Schengen Information System and Eurodac databases.[31]

The interoperability legislation contains provisions requiring the introduction of automated quality checks on all data entered in existing and forthcoming EU databases and information systems.[32] How those checks will be enacted will be set out in another piece of implementing legislation, which is also currently under discussion.[33]

This may go some way to solving problems caused by poor quality data, but will not happen for some time. In the meantime, there has been no suggestion of providing extra funding for national data protection authorities responsible for overseeing the use of these systems, despite previous calls for more funding and personnel in order to ensure effective supervision.[34]

Current and future checks for visa and travel authorisation applications

	Visa applications		Travel authorisation applications
	Current checks	Future checks	Future checks
National databases	X	X	X
EU databases			
Visa Information System			
Previous applications	X	X	X
Profiling tool		X	X
Schengen Information System			
Refusal of entry or stay	X	X	X
Surrender or extradition		X	X
Missing persons		X	
Wanted to assist with a judicial procedure		X	
Discreet checks		X	
Specific checks		X	
Lost or stolen travel document	X	X	X
Entry/Exit System			
Previous border crossings		X	X
Time spent within the Schengen area		X	X
European Travel Information and Authorisation System			
Previous travel authorisation application(s)		X	X
Watchlist		X	X
Eurodac			
Previous asylum application(s)		X	X
Irregular border crossing(s)		X	X
Apprehended in an irregular situation within the EU		X	X
European Criminal Records Information System for Third-Country Nationals			
Conviction(s) in EU for terrorism or other serious crimes		X	X
Multiple Identity Detector		X	X
Europol data		X	X
International databases			
Interpol			
Stolen and Lost Travel Documents database		X	X
Travel Documents Associated With Notices database		X	X



AUTOMATED PROFILING OF ALL TRAVELLERS

EU law defines profiling as using the automated processing of personal data "to evaluate certain personal aspects relating to a natural person". This can include analysing or trying to predict "performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." It is widely used in sectors such as insurance, finance and advertising and is becoming increasingly common in welfare, migration and security policy, to try to detect "'unknown' individuals who may be of interest" and aid in decision-making.[35]

The use of profiling raises serious risks for fundamental rights regarding discrimination, privacy and due process. Actions taken on the basis of profiling may lead to further interferences with the rights to liberty and security, to a family life, freedom of expression and freedom of assembly, amongst other things. In the context of migration policy, it may lead to inaccurate decisions or unwarranted searches, seizures, questioning or investigation. Any "bias, error, or system failure can result in irreparable harm to individuals and their families,"[36] who, as non-citizens, may face particular difficulties in exercising their rights to redress.

In the coming years, profiling will aid decision-making on both visa and travel authorisation applications and could be used to 'flag' individuals considered of further interest to the authorities. Data mining tools will comb through applications, statistics on overstay and refusal of entry, information from national authorities on security risks, and epidemic disease risks identified by global health bodies, in order to generate "screening rules". These will then be used to identify individuals previously unknown to the authorities, but "assumed to be of interest for irregular migration, security or public health purposes due to fact that they display particular category traits."[37]

In the legislation on visas and travel authorisations these category traits are referred to as "risk indicators". They include age range, nationality, country and city of residence, destination, purpose of travel and occupation. It is important to note that the rules and risk indicators used to assess visa and travel authorisation applicants will be based on data collected and analysed not solely by computers, but by people as well. "Bias may be introduced at each step of the process,"[38] increasing the risk of unwarranted refusals of applications, discrimination or invasions of privacy.

Such systems are already in use elsewhere. In February this year, Eyal Weizman, a researcher who investigates war crimes and state violence, was "barred from traveling to the United States for an exhibition of his work after being identified as a security risk by an algorithm used by the Department of Homeland Security." Weizman said he was given "no reason" for the refusal and officials at the US embassy in London asked him if he could think of any reason why the system had flagged him. An official asked for "the names of anyone in my network whom I believed might have triggered the algorithm."[39] As warned in a report on the use of automated decision-making tools for immigration and asylum purposes in Canada, there is the danger of creating "a laboratory for high-risk experiments within an already highly discretionary system."[40]

In fact, the EU has been such a laboratory for quite some time. In 2016, a piece of legislation called the Passenger Name Record (PNR) Directive introduced the first automated profiling system in the EU's border control regime.[41] This requires almost all airlines[42] to hand over data on all passengers on flights travelling into, within or out of the EU to 'Passenger Information Units' run by national law enforcement authorities. The data is compared against national and EU databases and against "pre-determined criteria" – a phrase seemingly-analogous to "risk indicators" – in order to detect individuals of interest prior to their arrival at an airport. The rules are being challenged in court by the *Gesellschaft für Freiheitsrechte* (Civil Rights Association, based in Germany) and *epicenter.works* (based in Austria).[43]

Meanwhile, the UK government has in recent years quietly introduced an automated profiling tool into its visa application system (the UK was never a Schengen state and so has always had a separate visa regime). The digital rights organisation *Foxglove* and the *Joint Council for the Welfare of Immigrants* are challenging the use of the "streaming tool" that is used to sift applications into "a fast lane (Green), a slow lane (Yellow), or a full digital pat-down (Red)." The two groups are pursuing a judicial review to find out what exactly the system does, how it works, and make sure it complies with the law. "As far as we can tell," say Foxglove, "the algorithm is using problematic and biased criteria, like nationality, to choose which "stream" you get in. People from rich white countries get "Speedy Boarding"; poorer people of colour get pushed to the back of the queue."[44]

It can be observed that the introduction of these systems represents, in some respects, the technological enforcement of already-existing practices. For example, EU states have long-deployed immigration liaison officers abroad to profile passengers and prevent them boarding flights if they are deemed likely to seek asylum, and countries in the Balkans have been pressured into preventing their own nationals, if they are deemed to fit a certain profile, from departing their territory.[45]

Decisions based solely on automated profiling are illegal, but automated systems may exert significant influence on official decision-making, as has been found with police use of facial recognition technology.[46] Further legislation is being drafted to establish the details of the profiling systems for the VIS and the ETIAS. Close scrutiny should be afforded to that legislation and the use of the systems, which may have profound implications for the tens of millions of people who travel to the EU every year.

A NEW PRE-CRIME 'WATCHLIST'

The inclusion of wanted or suspect individuals on lists drawn up by the police or other authorities is an old phenomenon. However, digital technologies make it far easier to maintain and extend such lists, and the EU has several of them. The Schengen Information System (SIS), for example, contained alerts on over 126,000 persons wanted for "discreet" or "specific" checks at the end of 2019.[47] In the case of the former, border guards or other officials surreptitiously gather as much information as possible from an individual, without making them aware they are the subject of an alert. The latter type of check involves direct questioning by border guards or other officials. Europol can also store data on 'potential criminals'. The EU also maintains lists of individuals subject to sanctions, such as asset-freezing, due to their involvement in acts of terrorism.[48]

The keeping of such lists can be lawful, but raises a number of serious questions concerning fundamental rights. The EU's terrorism 'blacklists' were the subject of serious criticism due to the listing process and the failure to provide basic procedural rights, such as the possibility of appeal, until a series of high-profile legal cases led to some changes.[49] A large number of authorities are able to insert alerts in the SIS – primarily law enforcement, judicial and border authorities, but also intelligence agencies and bodies from non-EU countries.[50] This raises questions about oversight, to ensure that alerts are justified and accurate, and may make it difficult for individuals to exercise the limited rights available to them when they are subject to "discreet" or "specific" checks.

The legislation on ETIAS establishes a new watchlist,[51] against which all applications for travel authorisations and, under legal proposals being discussed, visas,[52] will be checked. On the one hand, this list will include data on individuals who are suspected of having committed or taken part in terrorist or other serious criminal offences. On the other, it will include people who it is believed may commit such offences in the future. In this respect, it is "future-oriented" and aims to "support decision-making on who is authorised to travel to the EU based on what a traveller might do," not only what they may have done.[53]

Both Europol and EU member state authorities will be able to enter information into this new watchlist. The authority that enters the data is responsible for ensuring it is "adequate, accurate and important enough to be included."[54] Individuals will have the right to request access to and correction or deletion of any data held on them by EU and national authorities, but the process may not be simple. A variety of different data protection regimes will govern the watchlist and its use.[55] Law enforcement authorities, responsible for data added to the list, have ample opportunities to apply restrictions to data subjects' rights. More fundamentally, no EU institution has ever publicly explained why the watchlist is necessary and how it will relate to other existing EU systems, in which it is already possible to include the 'potential criminals' the authorities believe may commit offences in the future.

Some further legislation will be passed to clarify the "technical specifications" of the watchlist.[56] As with the forthcoming traveller profiling system, this legislation and the eventual use of the watchlist should be closely scrutinised to examine its impact upon fundamental rights.

MAKING A DECISION

VISAS

These new methods of processing visa applications will be far more data-intensive than is currently the case, but should – in theory – be far quicker. The aim is to produce better-informed decisions more swiftly and introduce a 'level playing field' in the assessment of visa applications across the Schengen states.

However, there is no guarantee these new technologies will achieve their goal. A 2013 study found that for citizens of eastern and central European states and "oil-rich countries," except Iraq and Iran, "not receiving the visa applied for is a rare experience." On the other hand, despite applying for a relatively low number of visas, citizens of sub-Saharan African states faced an "extremely high" refusal rate. The most recent statistics demonstrate the same trend.[57]

The same study highlighted that for western Schengen states such as France and the Netherlands, visa issuance and refusal patterns "are highly sensitive both to the country's postcolonial legacies and general economic interest in regard to emerging economies, while new [Schengen] members are, with very few exceptions, acting nearly exclusively in relation to non-EU Eastern European countries." If the data fed into the EU's new automated systems is skewed by political and economic interests and colonial legacies – not to mention the discretion of officials, who make the final decision on visa applications[58] – then the 'risks' that they indicate will be equally flawed. At the same time, as noted previously, the introduction of new automated checks may actually slow down the procedure, by introducing more data that has to be manually verified by officials.

The political, economic and historical interests at play in the visa procedure are well-demonstrated by a further facet of the Schengen regime. Individuals of certain nationalities are subject to more stringent checks than others, through a process known as 'prior consultation'. Any EU member state can notify all other member states that if an individual of a particular nationality applies for a visa, the notifying member state must be consulted by the consulate that has received the application. The consulted state has a veto power over the decision to issue the visa or not.

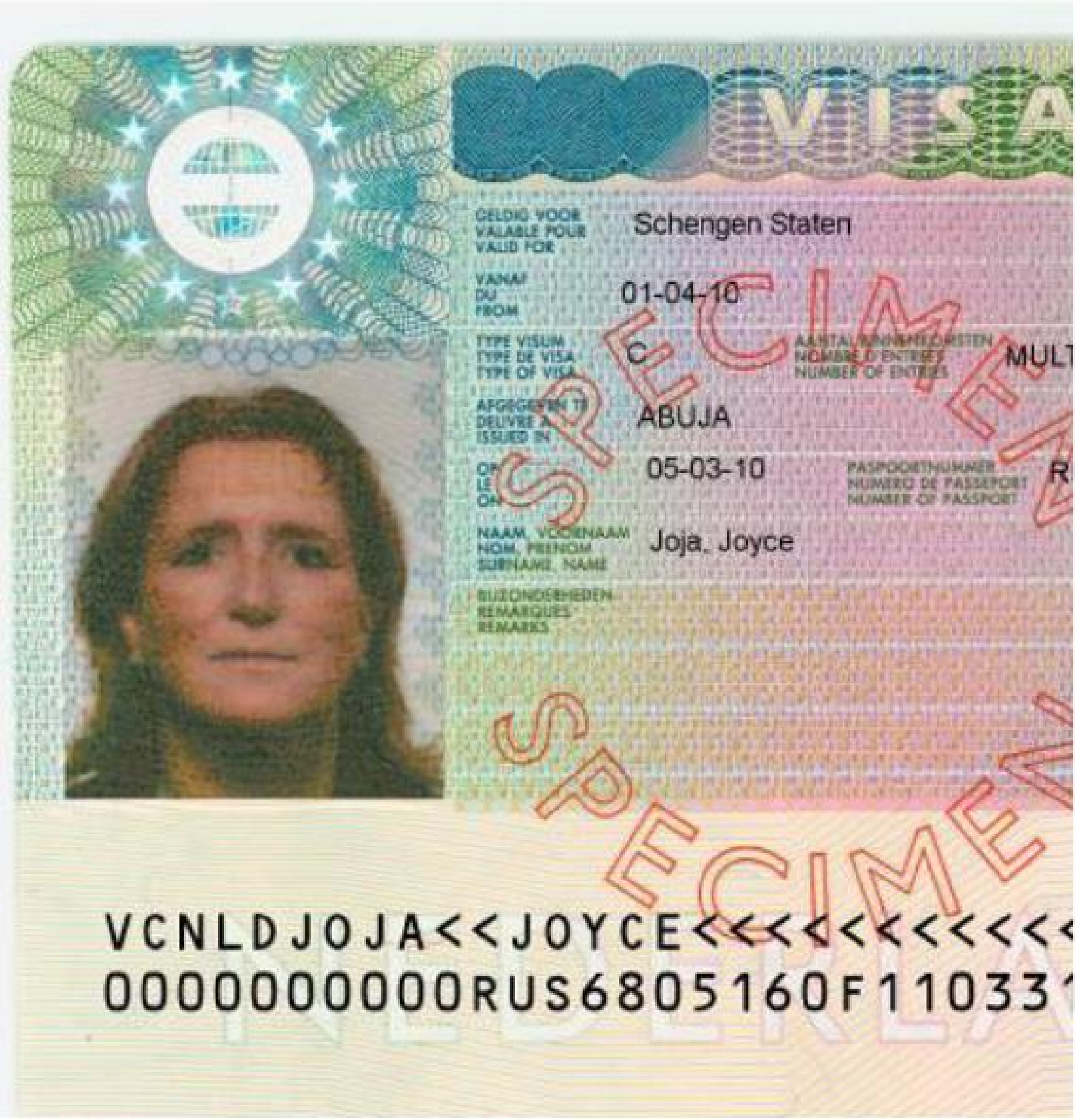
A US diplomatic cable released by Wikileaks in 2004 provides a vivid illustration of the way this works. The cable, from the US embassy in Brussels, said that the nationalities subject to prior consultation "generally follow colonial patterns. For instance, before any member state issues a visa to an Algerian citizen, France must be given the name of the applicant." If the authorities so decide, "France can refuse to allow the partner Member State to issue the visa."[59]

The list of nationalities (and specific categories of person holding that nationality, for example diplomats) subject to prior consultation is published, although the particular member states that require prior consultation remain secret. There are currently 38 states on the list – over a third of all the states whose citizens require a visa to enter the Schengen area. Moreover, any refugee or stateless person who applies for a visa, whatever their nationality, also faces 'prior consultation'.

The end result of all these checks and consultations is, of course, the issuance or refusal of a visa. This must be done within 15 calendar days from the date on which the application was lodged, but can be extended to up to 30 or even 60 days. With a visa affixed to their passport, an individual will then be able to travel to the Schengen area.

TRAVEL AUTHORISATIONS

A travel authorisation is issued if all the checks and procedures put in place show no indication of a security, illegal immigration or high epidemic risk. Applicants should be informed of the result within 96 hours of making an application, but this can be extended if additional information or documentation is requested, or if they are called to an interview at a member state's consulate. Once an application has been approved, the traveller will be able to make their journey to the Schengen area.



VISA

GELDIG VOOR
VALABLE POUR
VALID FOR — Schengen Staten

VANAF
DU
FROM — 01-04-10

TYPE VISUM
TYPE DE VISA
TYPE OF VISA — C

AANTAL BINNENKOMSTEN
NOMBRE D'ENTREES
NUMBER OF ENTRIES — MULT

AFGEGEVEN TE
DELIVRE A
ISSUED IN — ABUJA

OP
LE
ON — 05-03-10

PASPOORTNUMMER
NUMERO DE PASSEPORT
NUMBER OF PASSPORT — R

NAAM, VOORNAAM
NOM, PRENOM
SURNAME, NAME — Joja, Joyce

BIJZONDERHEDEN
REMARQUES
REMARKS

SPECIMEN

```
VCNLDJOJA<<JOYCE<<<<<<<<<<<
0000000000RUS6805160F11033
```

A Schengen visa.

SOURCE: EUROPEAN COMMISSION

STEP TWO:

THE JOURNEY

Since the 1980s, European and other states have sought to prevent certain categories of person, in particular asylum-seekers, arriving on their territory. A key method for doing so has been the introduction of 'carrier sanctions' – penalties against travel companies ('carriers') that transport people without the correct papers.[60]

Carrier sanctions have been heavily criticised for privatising immigration control measures, as they require that private companies take on the type of task traditionally reserved for public authorities. They are a key reason so many refugees arrive in the EU on foot or in unseaworthy boats – they cannot acquire visas and so cannot travel by plane, bus or any other means reserved for 'bona fide' travellers.[61] For individuals who have managed to acquire a visa or, in the future, a travel authorisation, checks carried out by travel companies represent another link in the chain of control that is being extended to all categories of 'legitimate' traveller.

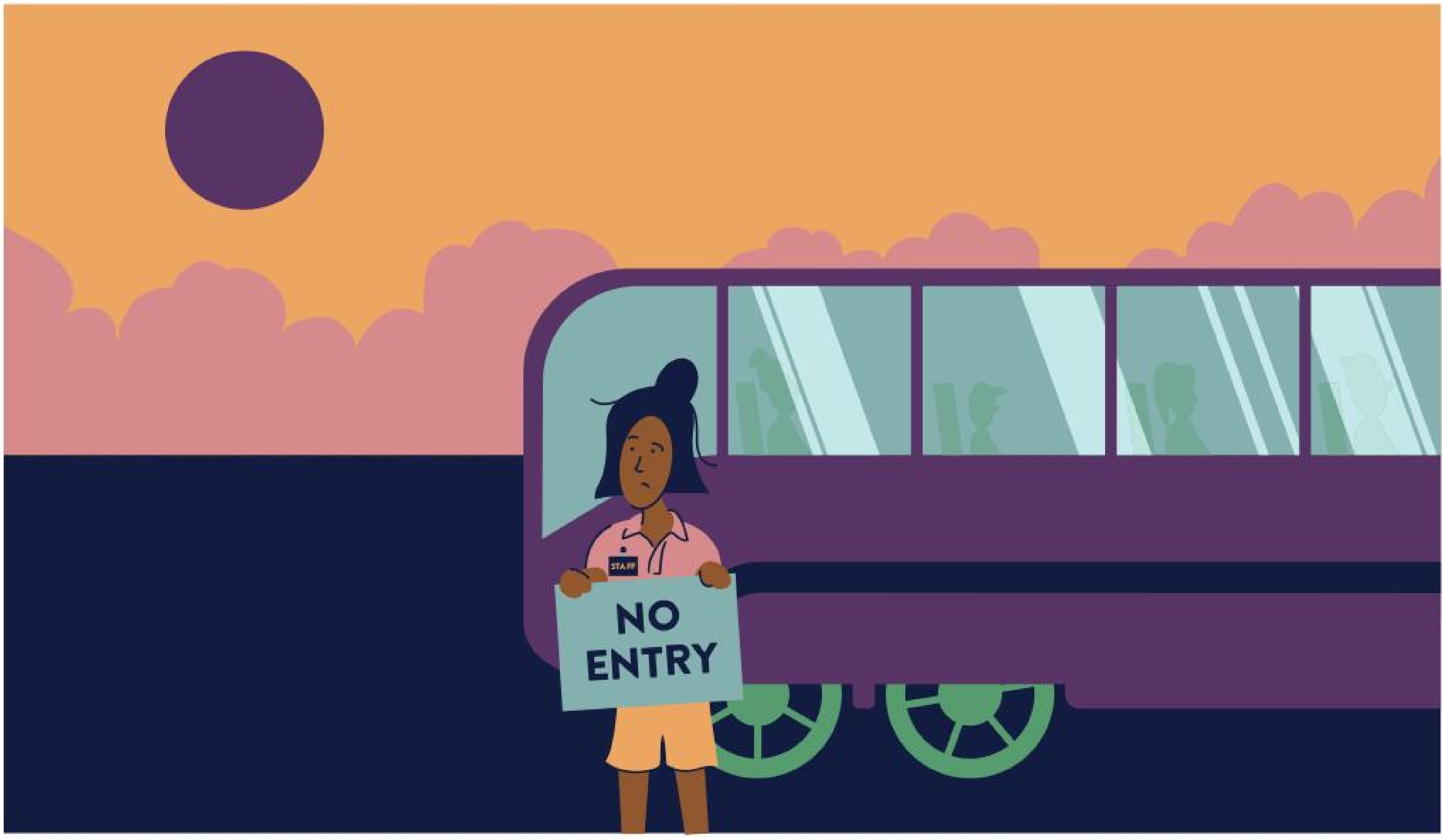
Carriers can already make phone calls to check the validity of visas held by people travelling to the Schengen area. In the future, this process will be simplified and travel authorisations will be subject to similar checks. When the revamped VIS and the ETIAS come into use, airline, ferry and coach companies will be given access to the systems' central databases to verify whether passengers have a valid visa or travel authorisation or not, although they will not be able to see any of the data held in the systems.

Travel companies will have to enter a passenger's name and travel document details (such as number and issuing country) into an online portal, which may be done by scanning the machine-readable zone on their passport or travel document. This will send the information to the central database of either the VIS or the ETIAS, which will send one of two responses: 'OK', or 'NOT OK'.[62]

The following step is simple enough: travellers who are OK will be allowed to board; those who are NOT OK will not. However, if a company allows an individual whose details trigger a NOT OK message to board – whether wilfully, or by a failure to check – they can be fined by the state to which they are travelling, or even punished by confiscation of property or withdrawal of transport licences. There is no systematic data on the application of carrier sanctions, but recent research suggests fines across the EU member states reach millions of euros every year.[63]

Carriers are also responsible for taking back those 'NOT OK' passengers they have transported, leading to further costs for the companies. For the individual, refusal of passage will undoubtedly have a financial impact – such as wasted travel tickets – but may have far more serious, unquantifiable costs, such as inability to see a loved one or, in the most serious cases, inability to find a place of refuge.

If a visa or travel authorisation holder travels to the Schengen area by plane, a separate set of personal data will also be shared with law enforcement authorities. As noted previously, under the Passenger Name Record (PNR) Directive, this data will be handed to a 'Passenger Information Unit' for checks against national, European and international databases and for use in a profiling system. It is likely that there will be demands to extend this system to boat, rail and coach travel in the future.[64] A pilot project between Belgium, France, the Netherlands and the UK is currently examining the use of such a system for high-speed train travel.[65]



STEP THREE:

AT THE BORDER

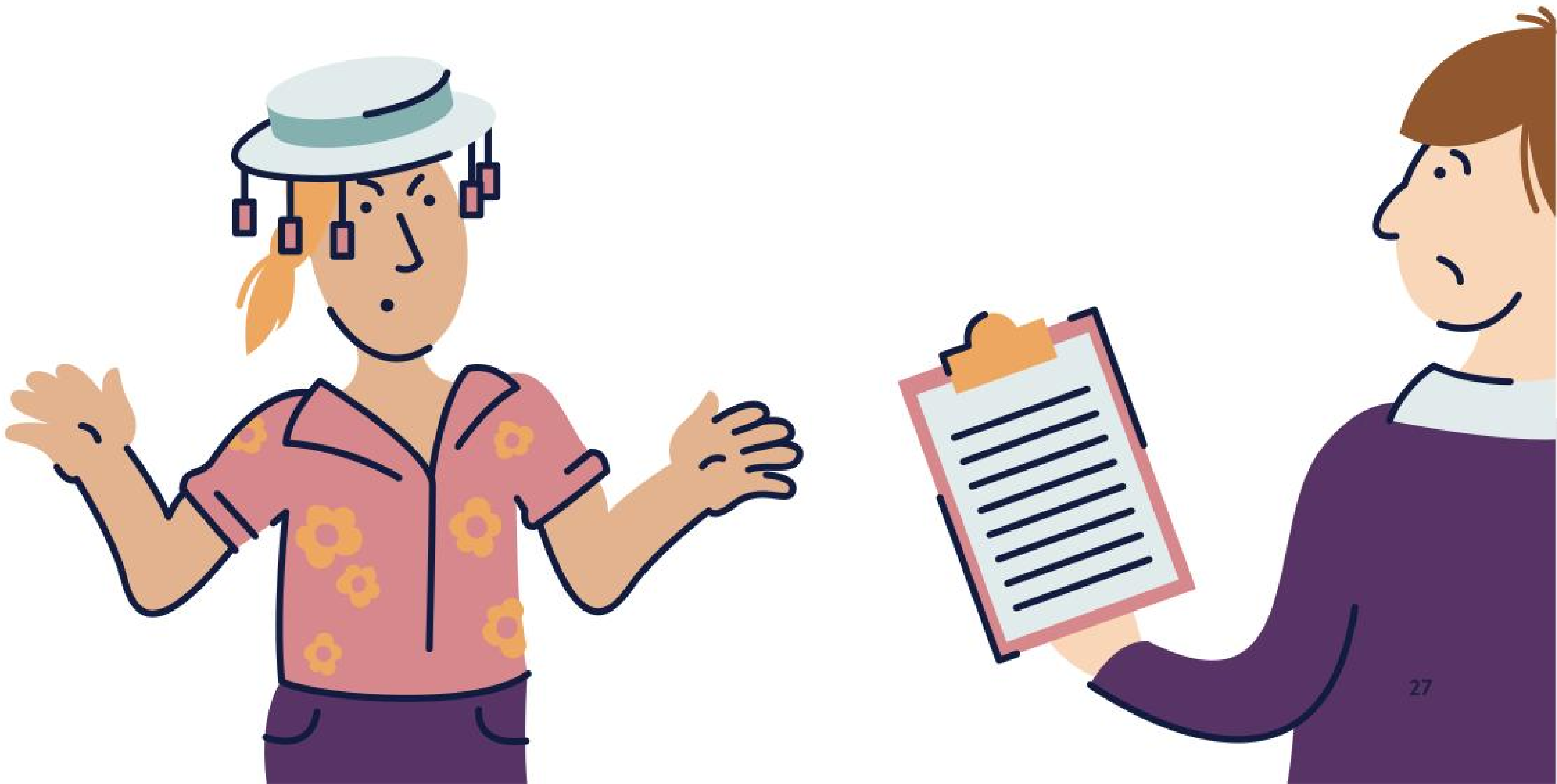
Once an individual arrives at the border – whether that be in France, Spain, Sweden, Poland or any other Schengen state – their personal data will begin another journey around the EU's digital circuits of security. Everyone crossing the external borders of the Schengen area is supposed to be checked against the Schengen Information System, as well as national and Interpol databases of lost and stolen travel documents. As of March 2017, EU citizens are also supposed to be subject to such checks, indicating that EU citizenship is no guarantee against being considered inherently suspicious.[66]

There are other checks – visa holders will have their identity checked against the VIS, and travel authorisation holders against the ETIAS. Travel authorisation holders will have four fingerprints and a photograph taken upon arrival at the border, for inclusion in the Entry/Exit System database, whereas visa holders will already have had 10 fingerprints and a photo taken as part of the visa application process.

Both categories of traveller will have their border crossing registered in the Entry/Exit System (EES), when that system comes into use, which is currently planned for the end of 2021. The EES will be used for the biometric registration of all border crossings in an individual file, and to see whether non-EU citizens entering the Schengen area have previously stayed longer than permitted. If so, they may be subject to refusal of entry and their data will be held in the EES for three years. Under legislation approved in late 2019, officials from the Frontex 'standing corps' of border guards, as well as national officials, can be made responsible for carrying out border checks and refusing or granting entry.[67]

More traditional methods of inquiry can also be used. For example, border guards are supposed to verify an individual's point of departure and destination, the purpose of their journey and whether they have means of subsistence for their intended trip. An individual's documentation and baggage may be inspected for these purposes, as well as to ensure that they are not a potential danger to public security.[68]

Travel authorisation holders may also be marked for closer inspection. "In cases where there is doubt as to whether sufficient reasons to refuse the travel authorisation exist," national officials responsible for examining applications can add a 'flag' to a file.[69] A border guard checking their identity against the ETIAS database at the border will see this flag and should then call them aside for further questioning. These flags may be added to individuals' files because the profiling system has identified them as a potential 'risk', leading to the possibility of unwarranted or discriminatory interviews or searches.



STEP FOUR:

IN THE SCHENGEN AREA

A traveller might be visiting the Schengen area for any number of reasons: a holiday in the Mediterranean; a business trip to Slovenia; seeing friends or relatives in the Netherlands; a wedding in Poland… Unless they are engaging in some kind of suspicious or unlawful activity, they should be free to enjoy their time as they wish. However, as has been widely documented over the years by civil rights organisations, we are not all equal before the law. Ethnic profiling by law enforcement officials means that people with darker skin are more likely to be targeted for identity checks and searches than their 'white' counterparts. Travellers with ethnic origins in Africa or the Middle East are particularly likely to come in for scrutiny.

As the Open Society Foundations have explained, police or other law enforcement officers "engage in ethnic profiling when they base their actions on ethnicity, race, religion, or national origin instead of an individual's conduct or objective evidence," which is illegal under both EU and international law. The organisation has documented widespread ethnic profiling in Bulgaria, France, Hungary and Spain;[70] the practice is also well-documented in the UK[71] and Germany,[72] amongst other places. This practice can just as easily take place at borders as it can within the territory of the EU, and while it is not limited to state officials, the power they wield means that ethnic profiling has particularly serious effects when it informs their work.

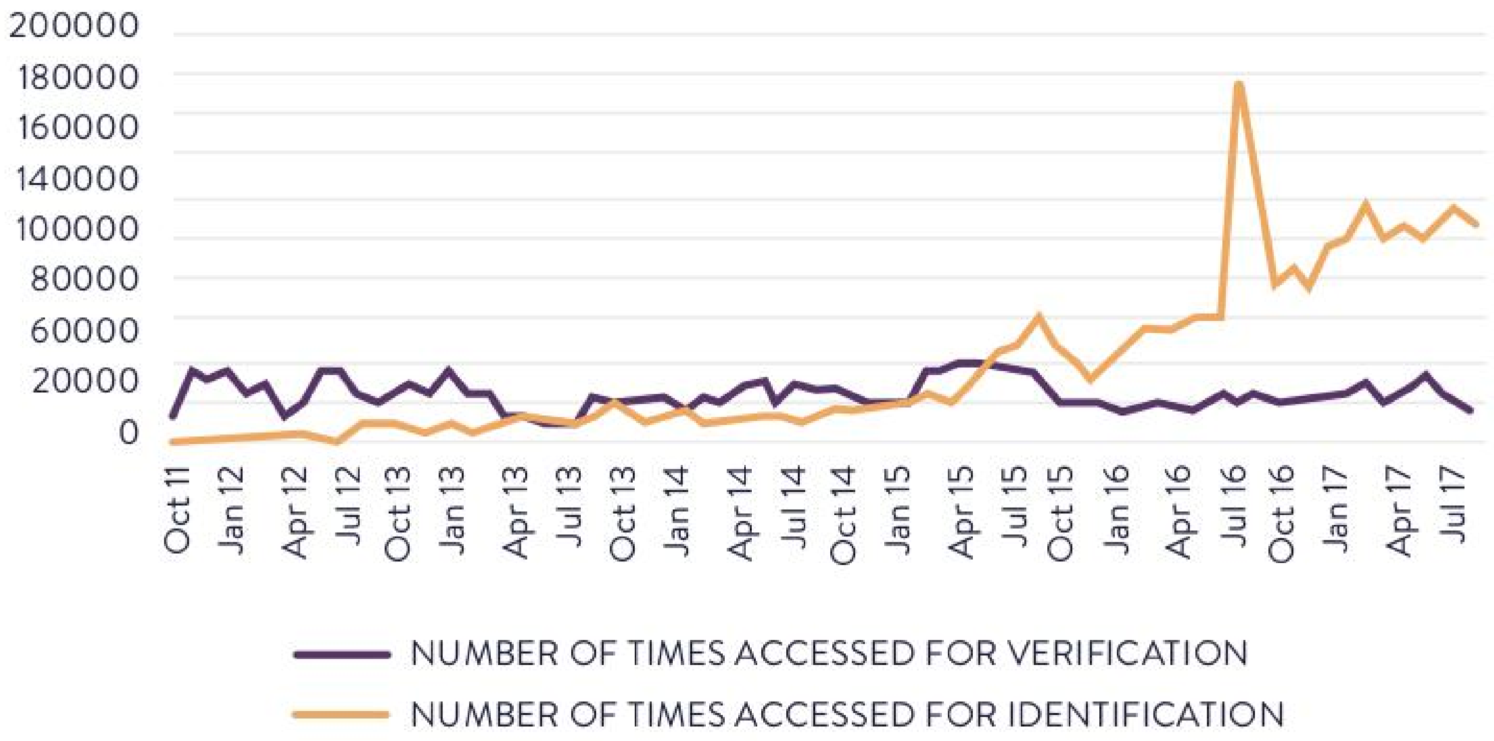
As noted earlier, in the years to come, the 'identity data' of non-EU nationals – names, date and place of birth, sex, travel document data, fingerprints and a photograph – will be extracted from five individual large-scale databases and stored in a new system called the Common Identity Repository (CIR). The purpose of the CIR is to facilitate police identity checks, by providing a common pool of biometric and biographic data on the vast majority of non-EU nationals present in the Schengen area. By encouraging an increase in identity checks, the introduction of the CIR will indirectly encourage an increase in ethnic profiling.

The VIS is already used for carrying out identity checks, and such usage has increased steadily over the years (see chart). National authorities responsible for checking "whether the conditions for entry to, stay or residence in the territory of the Member States are fulfilled," can search the VIS using the visa number and/or an individual's fingerprints. This can be done to verify their identity (to see whether the person in possession of the visa is the same person whose data is stored in the database) or to try to identify them (in cases where they are not in possession of a visa, but an official has reason to believe their data may be stored in the VIS). Similar legal provisions exist for the ETIAS and EES databases.

The rules on using the CIR for identity checks are far more permissive. There is no requirement for an official to be checking whether the conditions for being in the Schengen area are fulfilled. Instead, the database will be accessible when an individual does not have an identity document, when there are "doubts" about the identity data provided by an individual, the authenticity of an identity document or the identity of a document holder, or when a person is unable or refuses to cooperate. National law will govern these checks, with only very limited safeguards contained in the EU legislation itself. Any other actions taken by the authorities – for example searches, questioning, or detention – will also be governed by national law.

If an official carrying out an identity check is authorised to access both the CIR and the VIS, both the CIR and the ETIAS, or both the CIR and the EES, they will be given access to more than just an individual's identity data when a search in the CIR leads to a 'hit'. In the case of visa holders, a police officer would be able to see all the data from their application form, the photograph and the validity period of the visa. In the case of travel authorisation holders, an official carrying out an identity check will be told if the authorisation is valid, for which member state (in the case of an authorisation of limited territorial validity), and the remaining validity period. In the case of the EES, access will be granted to the individual's file in that system and the entry and exit records associated with it.

USE OF THE VIS WITHIN THE SCHENGEN AREA



The use of the Visa Information System for verification and identification within the Schengen area.

SOURCE: EU-LISA

STEP FIVE:

DEPARTURE

Anyone leaving the Schengen area is supposed to be subject to the same checks as upon entry. Visa and travel authorisation holders will, upon their departure, have their personal data whisked through various national, EU and international databases and information systems in order to ensure that they or their travel document have not become subject to a law enforcement alert during their stay.

Data on all visa and travel authorisation holders is stored for quite some time. In the case of visas, from the moment a file is created in the VIS, it will be held for five years. In the case of travel authorisations, once granted they will be valid for three years (unless the travel document they are attached to expires before that point) and the holder can give their consent to its storage for a further three years, to make repeat applications more straightforward. If an authorisation is refused, annulled, or revoked, it will be stored in the central ETIAS database for five years. Both visa and travel authorisation holders will also have files on them stored in the Entry/Exit System. These will be stored for three years (including on individuals refused entry), unless there is no record of exit, in which case the data will be held for five years while the authorities attempt to track down the 'overstayer'.

These retention periods are likely to be particularly useful for the new profiling tools being introduced into the visa and travel authorisation systems, by ensuring an extensive set of data is held at any given moment. The profiling tools will be based in large part on the automated data-mining of statistics and information on visas, travel authorisations, entry/exit records and other EU and national sources. One critical assessment of the ETIAS argued that a profiling system was being introduced not because of any clear need for it, but "simply because the volume of data ETIAS will hold happens to allow such profiling."[73] The longer the retention period, the greater the volume of data. Data held in the VIS, ETIAS and EES will also be accessible to Frontex, so that agency can conduct "risk analysis" and "vulnerability assessments".

Data held in the VIS, ETIAS and EES will be accessible to law enforcement authorities conducting criminal investigations, under certain conditions, and lengthy retention periods are certainly useful for that purpose. Criminal investigators can access the VIS if it is necessary in a specific case and there are reasonable grounds to believe that access will "substantially contribute to the prevention, detection or investigation of any of the criminal offences in question."[74] The most recent data available shows that law enforcement usage of the VIS increased by some 500% between 2013 and 2017, from 500 to over 2,500 searches annually.

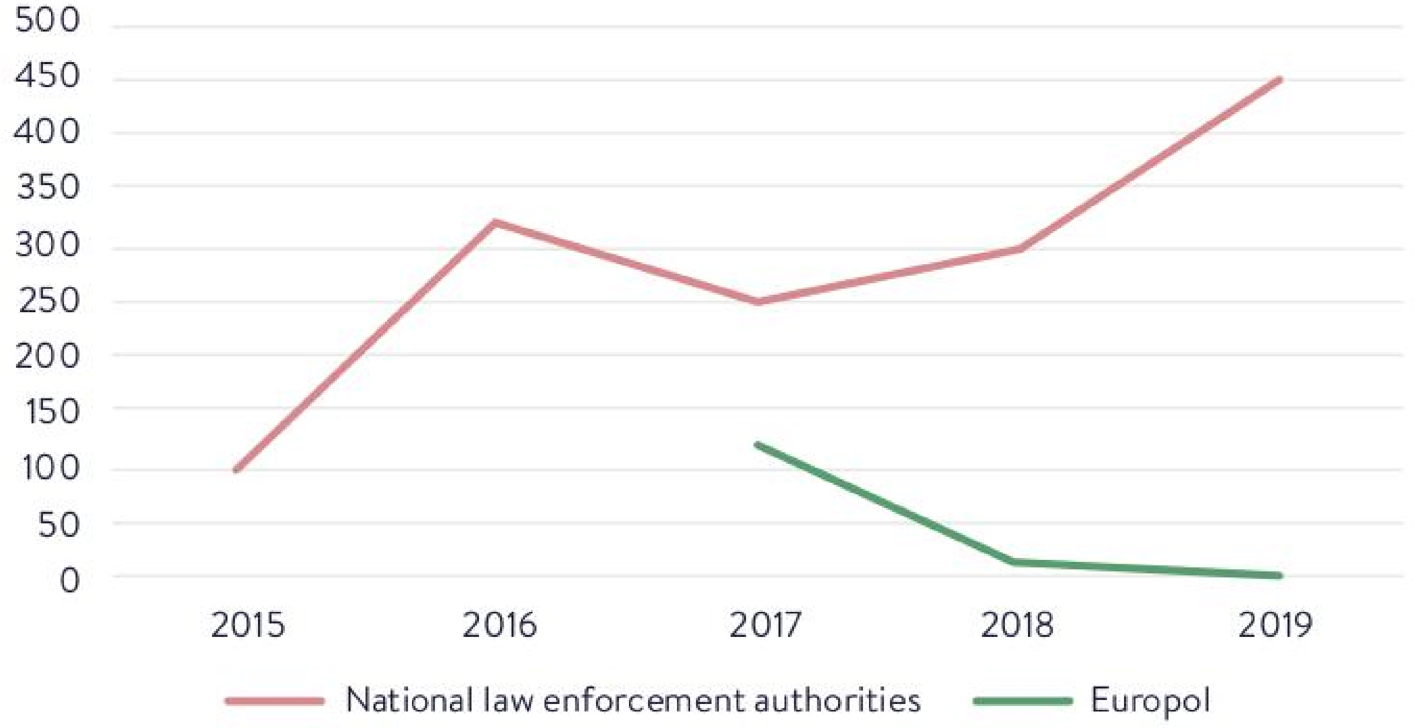
Although the possibility of law enforcement agencies accessing the non-policing data held in the EU's migration and asylum databases has become a standard feature of those systems, it has proven controversial in the past. The rules on access to the VIS were passed in 2008 by EU governments alone, as the European Parliament had no say on policing matters until the entry into force of the Lisbon Treaty in 2009.

When in May 2012 a proposal came before the Parliament to allow law enforcement access to the Eurodac database of asylum-seekers' fingerprints, it provoked uproar amongst MEPs, refugee rights campaigners and data protection specialists. They argued that the proposals were neither necessary nor proportionate and that they "may result in the stigmatisation of asylum-seekers as a group by associating them with criminal activity."[75]

Nevertheless, the measures were approved and law enforcement searches became possible as of July 2015. Since then, usage has increased somewhat, but the number of searches – 449 in 2019 – does little to support the claim made by proponents of the changes that there was an urgent need to give police access to the Eurodac database. Neither is there any way to know if access to this data is actually useful for policing purposes, due to a lack of data collection and empirical analysis.

Granting law enforcement agencies the possibility to access EU databases on non-EU citizens has thus become standard practice. The European Commission initially argued that there was no evidence to support the need for such access to the EES,[76] but it was overruled by the member states.[77] By the time the ETIAS legislation was proposed, it appeared that the European Commission had got the message, and the possibility of law enforcement access was included from the start.[78]

LAW ENFORCEMENT USE OF EURODAC



CONCLUSIONS: YOUR PERSONAL DATA IS GOING ON A JOURNEY

The EU is constructing a number of new systems for the screening, monitoring and tracking of international travellers that places them under an increasing veil of suspicion. Justified primarily in the name of ensuring security, all non-EU citizens attempting to visit the Schengen area will have their biometric and biographic data registered in large centralised databases, where it will be cross-referenced against a host of other systems and used to feed new databases, profiling tools and watchlists and used for a multitude of purposes beyond the processing of visa and travel authorisation applications. This raises a number of immediate and more long-term concerns that require further investigation, reflection and action.

EXTENDED DATA-GATHERING AND PROCESSING

The process of making an application for both visas and travel authorisations will require the collection of more personal data from a far greater number of people than at present. While the forthcoming rules on visa applications do not introduce significant new categories of personal data to the system, they will vastly expand their scope, by lowering the age limit for fingerprinting to just six years old. The biometric data of up to a million more children will be stored as part of the visa process. The rules on travel authorisations, meanwhile, require the collection of various types of personal data from travellers who currently are not subject to any such regime, including on their education, employment, criminal records and more.

FEEDING A NEW IDENTITY DATABASE

The mere collection and storage of any personal data has to be necessary and proportionate if it is to be considered legitimate. However, the new troves of data that will be held on visa and travel authorisation applicants are also intended to undergo significant further processing. 'Identity data' – names, date and place of birth, sex, travel document data, fingerprints and a photograph – are to be stored in a vast new database, the Common Identity Repository (CIR), which is being introduced to facilitate police identity checks within the EU and to ease the use of other new technologies, such as the forthcoming Multiple Identity Detector (MID). This is just one of an array of tools that are being introduced in order to judge whether travellers are 'risky' or not.

AUTOMATED DATABASE CHECKS

In a significant departure from current practice, there will be automated checks of all visa and travel authorisation applicants against a wide variety of national, EU and international databases concerning asylum policy, criminal records registries, police alerts, lost and stolen documents and border crossings, amongst other things, while automated checks through the Multiple Identity Detector will try to establish whether a false identity is being used. Whether these new procedures will yield a significant number of results remains to be seen. However, it is important to note that, for travel authorisation applicants in particular, this is a fundamental shift to being treated *a priori* as potential suspects. Furthermore, it has been well-demonstrated that Interpol's systems for reporting lost and stolen travel documents have been widely-misused, and this provides a further opportunity for such nefarious activities. The fact that travel authorisations will be automatically refused if an individual's travel document is reported as lost or stolen with Interpol is an issue of particular concern.

AUTOMATED PROFILING AND THE RISK OF DISCRIMINATION

Perhaps the most troubling of all the new elements being introduced to the visa and travel authorisation procedure is the automated profiling system. The EU's Fundamental Rights Agency, commenting on the proposal to introduce the ETIAS, remarked that there is "limited research available on the feasibility of using risk indicators without engaging in discriminatory profiling," and that such a system should only be introduced if a test phase demonstrates the necessity and proportionality of doing so.[79] There has been no such caution in the approach adopted by the EU and the functioning of these systems must be subject to close scrutiny from public institutions and civil society.

'PRE-CRIME' WATCHLIST

A further dangerous novelty comes in the form of the new 'watchlist' being introduced for the ETIAS and the VIS, which will contain data on people suspected of having committed crimes in the past, as well as those who it is believed may commit crimes in the future. The watchlist is being introduced despite the EU already having a range of such options at its disposal: for example, by storing alerts in the SIS, in the data held by Europol, or on the terrorism sanctions lists it maintains. The need for this new system is unclear and the safeguards largely rely on law enforcement authorities checking their own practices. As with the profiling function, critical oversight and examination of the watchlist function will be required in the years to come.

OUTSOURCED BORDER CONTROLS

Once a visa or travel authorisation is accepted, the applicant will be able to travel to a Schengen border. The network of control that is exercised over potential visitors to the EU is also being expanded to this stage of the process. Carriers, such as airlines or coach companies, will serve as outsourced border guards, obliged to check all non-EU citizens' documents against the VIS and ETIAS databases to see whether their papers are in order. While this is not an entirely new role for travel companies, the introduction of new technologies and the expansion of 'permission to travel' requirements to non-EU citizens not subject to a visa obligation represent new links in the chain of scrutiny and control being placed upon non-EU citizens who wish to visit the Schengen area.

QUERIES AT THE BORDER

At the border, an individual's personal data will once again be screened against a panoply of national, EU and international databases and their personal data will be stored in another new database, the Entry/Exit System (EES). This will hold the biometric and biographic data of almost all visitors to the Schengen area and will be used to determine whether they have stayed longer than permitted. More traditional enquiries, such as questioning and searches, may also be made of travellers, but these too may be informed by new technologies. In particular, the function allowing officials who approve a travel authorisation to 'flag' an individual of interest to border guards may result in unwarranted or discriminatory questioning or searches at the EU's borders.

CHECKS IN THE SCHENGEN AREA

Within the Schengen area, these new databases will also play a role in the monitoring of travellers. The CIR is intended to facilitate police identity checks within the territory of the member states, and officials who are authorised to use the VIS, ETIAS and EES will also be given access to the underlying data held in those systems, such as data from a visa application file or travel authorisation. While the VIS, ETIAS and EES legislation allows for the use of the systems for identity checks, the rules governing the CIR are far more permissive and lack the necessary checks and balances that might help mitigate the use of the system as part of ethnic profiling operations. Indeed, the very existence of the CIR is likely to indirectly encourage the use of ethnic profiling in police work, as it will consist of a vast new dataset entirely on non-EU citizens. In combination with access to the VIS, ETIAS and/or EES, ordinary police officers will be granted access to a significant amount of data about a person, their travel history and their personal circumstances.

AFTER DEPARTURE

Even after an individual has left the Schengen area, their personal data will have a long afterlife. Files will remain in the VIS for five years, in the ETIAS for three years (with a possibility for a three-year extension, subject to the traveller's consent) and in the EES for three years (or five years if no exit is logged). These retention periods will ensure the availability of the necessary raw material – that is, personal data – for the construction of the profiling tools, may be accessed in the course of criminal investigations, and will be processed every time any other individual makes a visa or travel authorisation request, or the new Multiple Identity Detector is launched.

DATA QUALITY

A number of overarching issues accompany these changes. The first is that if these new systems are to function correctly, then it is of paramount importance to ensure that the data they use is accurate. However, it has been known for years that existing EU databases are riddled with errors, and it is only now – as new systems are under construction and existing ones are being expanded – that EU institutions and national governments are trying to work out ways to ensure high-quality, accurate data is entered and used. Combining the data of tens of millions of people in new databases, and cross-checking that data across a multitude of systems, massively increases the risk of errors that may result in irreparable harm to individuals.

DATA OVERLOAD

Secondly, it is also well-established that the authorities have trouble coping with the amount of data they have. There is no shortage of cases in which criminal acts – including terrorism – have been carried out by people already known to the authorities. The idea that more state storage of data will inherently keep us safe from potential 'threats' is severely lacking in credibility. The plans to vastly increase the storage of data on foreign nationals is also particularly worrying at a time when EU governments have shown themselves all too willing to subvert democratic norms and the rule of law whilst presenting foreigners as scapegoats for society's ills. There are huge potential dangers in the assumption that sensitive personal data on tens of millions of non-citizens can be centrally stored with no potential political risks in the years ahead.

NON-CITIZENS AS GUINEA PIGS

Thirdly, the technologies being deployed are untested, despite raising huge risks, in particular with regard to the potential for unlawful discrimination. Nowhere is this clearer than in the case of the profiling system being introduced for visa and travel authorisation applicants. Non-EU citizens will effectively be guinea pigs for a range of unproven tools and technologies that may lead to serious restrictions upon their fundamental rights. The fact that these new systems almost entirely concern only non-EU citizens is perhaps one reason why the use of dubious, untested technologies is taking place with so little public interest and scrutiny. The risk of 'population creep' – that is, extending the blanket gathering of biometric and biographic data for the purposes of risk analysis and monitoring of movement to EU citizens – should be a cause for more widespread critical attention.

ACCESS TO REMEDIES

A fourth overarching issue concerns the possibility of those affected by these systems to access an effective remedy. While the legislation contains all the relevant guarantees for data protection rights – such as to request access to one's own data and to have it corrected or deleted in case of error – the exercise of those rights may prove challenging. Numerous different data protection regimes (both EU and national) will govern the use of these systems. This will lead to significant legal complexity that will not be diminished by the fact that anyone seeking to exercise their rights will face a legal system with which they are unfamiliar and which functions in a language they may not speak fluently, if at all. Exactly how states will ensure that the rights provided on paper are effective in reality remains to be seen. Stringent oversight from national and EU data protection authorities will be needed to ensure access to those rights, as well as to ensure the systems are not abused, but there is no indication those authorities are being provided with significant extra resources for this work.

While, formally-speaking, there has been democratic scrutiny of the new rules, it is well-established that the EU's law-making process is largely opaque to all but those participating in it and unintelligible to non-specialists who do not have the time to accustom themselves to the jargon of 'trilogues' and 'comitology'. Over the last five years, EU policies on the processing of non-citizens' personal data have expanded and accelerated significantly, largely out of the public eye. Far greater scrutiny should be afforded to how these systems work in practice, as well as the development of future initiatives in this field.

ENDNOTES

1 Electronic System for Travel Authorization, electronic Travel Authorisation and Electronic Travel Authority, respectively.

2 Edward Hasbrouck, 'Government permission to travel: "Authority to Transport"', Papers, Please!, 8 February 2019, https://papersplease.org/wp/2019/02/08/government-permission-to-travel-authority-to-carry/

3 Long-stay visas are currently largely a national competence, although are increasingly coming within the scope of EU action. A number of changes are currently being introduced to the application process for long-stay visas. For example, the changes to the Visa Information System will expand its scope to include data on up to 22 million long-stay visa applications, as well as residence documents. However, this report only examines the changes that will be applied to short-stay visa applications. For some more information, see: 'All visa applicants to be profiled and children fingerprinted for revamped Visa Information System', Statewatch News, 17 August 2018, https://www.statewatch.org/news/2018/aug/vis-profiling-child-fingerprinting.htm

4 Statewatch has previously examined the potential impact of the 'interoperability' agenda on undocumented migrants present in the EU. See: 'Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status', Statewatch/PICUM, November 2019, https://www.statewatch.org/news/2019/nov/interoperability-report.htm

5 Margaritas Schinas, a member of Greece's conservative New Democracy party, is currently European Commissioner for Promoting our European Way of Life. When his job was first announced, it had the title "protecting our European way of life," a moniker that was roundly condemned and swiftly altered. The change of name has not, however, been accompanied by any change to the policy programme for which he is responsible. See: European Commission, 'Promoting our European way of life', https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life_en; David M. Herszenhorn and Maïa de La Baume, 'Outrage over 'protecting our European way of life' job title', Politico, 11 September 2019, https://www.politico.eu/article/outrage-over-protecting-our-european-way-of-life-job-title/

6 eu-Lisa, 'Technical reports on the functioning of VIS', May 2018, p.9, https://www.eulisa.europa.eu/Publications/Reports/2018%20VIS%20reports.pdf

7 Ibid., p.18

8 List of competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult data in the Visa Information System (VIS), Official Journal of the European Union, C 187/4, 26 May 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1591113452708&uri=CELEX:52016XC0526(01)

9 eu-Lisa, 'Technical reports on the functioning of VIS'

10 Deloitte/European Commission, 'Study on the feasibility and implications of options to digitalise visa processing', 10 February 2020, https://op.europa.eu/en/publication-detail/-/publication/4cb4fbb8-4c82-11ea-b8b7-01aa75ed71a1/language-en

11 Daniel Trilling, 'Scaled-up surveillance: the EU builds a massive biometric database', Coda, 9 June 2020, https://www.codastory.com/authoritarian-tech/eu-border-patrol-technology/

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

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

14 'Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status', https://www.statewatch.org/news/2019/nov/interoperability-report.htm

15 Ann-Charlotte Nygård, 'EU wide availability of personal data of third country nationals for migration and security purposes – the challenge of ensuring fundamental rights safeguards', Migration Policy Centre, undated, http://www.migrationpolicycentre.eu/eu-personal-data-third-country-nationals-for-migration-security/

16 Article 21, Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009R0810

17 Article 9a, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

18 Ibid.

19 The European Data Protection Supervisor, in an opinion on the legal proposals to revamp the VIS, did raise the issue of "the role and impact of data processed for law enforcement purposes in the visa issuance decision-making process," but did not fundamentally question the proposal's intentions. https://edps.europa.eu/sites/edp/files/publication/18-12-13_opinion_vis_en.pdf

20 Article 9c, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

21 Article 20, Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

22 Ibid.

23 Articles 22-27, Regulation (EU) 2018/1240, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

24 Elmas Topcu, 'Turkey using Interpol to track down dissidents', DW, 7 November 2019, https://www.dw.com/en/turkey-using-interpol-to-track-down-dissidents/a-51159723

25 Abdullah Bozkurt, 'Secret documents reveal abuse of Interpol mechanisms by Turkish government', Nordic Monitor, 1 February 2019, https://www.nordicmonitor.com/2019/02/secret-documents-reveal-abuse-of-interpol-mechanisms-by-turkey-government/

26 'Abuse of the Interpol system by Turkey', Stockholm Center for Freedom, September 2017, https://stockholmcf.org/wp-content/uploads/2017/09/Abuse-Of-The-Interpol-System-By-Turkey_September-20-2017.pdf

27 General Secretariat of the Council, 'Interoperability and the visa procedure – Possible implications of interoperability on the daily work of the consulates – Presentations', WK 8371/2019 INIT, 10 July 2019, http://statewatch.org/news/2019/aug/eu-counvcil-interop-visas-WK-8371-19.pdf

28 Commission Implementing Decision on the technical rules for creating links between data from different EU information systems, https://ec.europa.eu/transparency/regcomitology/index.cfm?do=search.documentdetail&Dos_ID=18686&ds_id=65379&version=1&page=1

29 Presidency of the Council, 'Structure and main principles of the roadmap for standardisation for data quality purposes – Presidency discussion paper', 7125/20, 15 April 2020, https://data.consilium.europa.eu/doc/document/ST-7125-2020-INIT/en/pdf

30 European Union Agency for Fundamental Rights, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights', 2018, p.96, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf

31 European Court of Auditors, 'EU information systems supporting border control – a strong tool, but more focus needed on timely and complete data', 2019, https://www.eca.europa.eu/Lists/ECADocuments/SR19_20/SR_Border_control_EN.pdf

32 Article 37, Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0817#d1e2990-27-1

33 Commission Implementing Decision laying down the details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data in the EES, VIS, ETIAS, SIS, the shared BMS and the CIR, pursuant to Article 37(4) of Regulation (EU) 2019/817 of the European Parliament and of the Council, https://ec.europa.eu/transparency/regcomitology/index.cfm?do=search.documentdetail&Dos_ID=18907&ds_id=66033&version=1&page=1

34 'Visa Information System: private companies gathering data, insufficient funding for data protection', Statewatch News, November 2015, http://database.statewatch.org/article.asp?aid=35780

35 European Union Agency for Fundamental Rights, 'Preventing unlawful profiling today and in the future: a guide', 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

36 Petra Molnar and Lex Gill, 'Bots at the gate: a human rights analysis of automated decision-making in Canada's immigration and refugee system', September 2018, p.4, https://citizenlab.ca/2018/09/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system/

37 Susie Alegre, Julien Jeandesboz, Niovi Vavoula, 'European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection', 18 May 2017, https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2017)583148

38 'Preventing unlawful profiling today and in the future: a guide', p.12

39 Robert Mackey, 'Homeland Security Algorithm Revokes U.S. Visa of War Crimes Investigator Eyal Weizman', The Intercept, 21 February 2020, https://theintercept.com/2020/02/20/homeland-security-algorithm-revokes-u-s-visa-war-crimes-investigator-eyal-weizman/

40 'Bots at the gate', p.1

41 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, https://eur-lex.europa.eu/eli/dir/2016/681/oj

42 ‘Private jets exempt from data collection law pose crime risk’, Investigate Europe, July 2018, https://www.investigate-europe.eu/en/2018/private-jets-exempt-from-data-collection-law-pose-crime-risk/

43 ‘No PNR’, https://nopnr.eu/en/home/

44 ‘Legal action to challenge Home Office use of secret algorithm to assess visa applications’, Foxglove, October 2019, https://www.foxglove.org.uk/news/legal-challenge-home-office-secret-algorithm-visas

45 Frances Webber, ‘The cradle or the grave? EU migration policy and human rights’, Statewatch Journal, vol. 23 no. 3/4, February 2014, http://database.statewatch.org/article.asp?aid=33154

46 A report on the use of automated facial recognition technology by the UK’s Metropolitan Police found that there was a “presumption to intervene” when the system in use detected a match between an image on a police list and an individual in the street. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

47 eu-Lisa, ‘SIS II – 2019 statistics’, March 2020, https://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20-%202019%20-%20Statistics.pdf

48 Consolidated text: Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02001E0931-20171115; Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002R0881

49 Gavin Sullivan and Ben Hayes, ‘Blacklisted: Targeted sanctions, preemptive security and fundamental rights’, 2009, http://www.statewatch.org/news/2010/dec/eu-ecchr-blacklisted-report.pdf

50 Matthias Monroy, ‘EU opens its biggest database for secret services from third countries’, 4 May 2020, https://digit.site36.net/2020/05/04/eu-opens-its-biggest-database-for-secret-services-from-third-countries/

51 Article 9a, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

52 Article 34, Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

53 https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2017)583148

54 Article 35(1)(a), Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

55 Personal data processing by member states’ law enforcement authorities is governed by national law and the EU’s ‘Law Enforcement Directive’ (Directive 2016/680). Personal data processing by Europol is governed by the Europol Regulation (2016/794) as well as Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies.

56 “The Commission shall, by means of implementing acts, establish the technical specifications of the ETIAS watchlist and of that assessment tool.” Article 35(7), Regulation (EU) 2018/1240, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

57 European Commission, ‘Complete statistics on short-stay visas issued by the Schengen States’, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-policy_en#stats

58 Francesca Zampagni, ‘Unpacking the Schengen Visa Regime. A Study on Bureaucrats and Discretion in an Italian Consulate’, Journal of Borderland Studies, 31(2), 2016, pp.251-266 https://doi.org/10.1080/08865655.2016.1174605

59 https://wikileaks.org/plusd/cables/04BRUSSELS4844_a.html

60 Erika Feller, ‘Carrier Sanctions and International Law’, International Journal of Refugee Law, 1(1), 1989, pp.48-66, https://academic.oup.com/ijrl/article-abstract/1/1/48/1578876?redirectedFrom=fulltext; The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0922(02); Council Directive 2001/51/EC of 28 June 2001 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001L0051

61 ‘Criminalising asylum: The EU adopts the French immigration proposals’, Statewatch News, August 2001, http://www.statewatch.org/news/2001/aug/13asylum.htm

62 Article 45(2), Regulation (EU) 2018/1240, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240; Article 45b(4), Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

63 Theodore Baird, ‘Carrier Sanctions in Europe: A Comparison of Trends in 10 Countries’, European Journal of Migration and Law, 19(3), 2017, pp.307-334, https://brill.com/view/journals/emil/19/3/article-p307_307.xml?language=en

64 ‘EU Council Presidency proposes follow-up on extending PNR to sea and rail traffic’, Statewatch News, 3 August 2019, http://www.statewatch.org/news/2019/aug/eu-pnr-all-borders-follow-up.htm

65 Heini Järvinen, ‘Belgium agrees on passenger controls of international rail traffic’, European Digital Rights, 8 February 2017, https://edri.org/belgium-agrees-passenger-controls-international-rail-traffic/

66 Council of the EU, ‘Schengen borders code: Council adopts regulation to reinforce checks at external borders’, 7 March 2017, https://www.consilium.europa.eu/en/press/press-releases/2017/03/07/regulation-reinforce-checks-external-borders/

67 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019R1896

68 Article 8(3), Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0399-20190611

69 Article 36(2), Regulation (EU) 2018/1240, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

70 ‘Ethnic Profiling: What It Is and Why It Must End’, Open Society Foundations, https://www.opensocietyfoundations.org/explainers/ethnic-profiling-what-it-and-why-it-must-end

71 Mark Townsend, ‘Racial bias in police stop and search getting worse, report reveals’, The Guardian, 13 October 2018, https://www.theguardian.com/law/2018/oct/13/racial-bias-police-stop-and-search-policy-black-people-report

72 ‘Germany: UN rights panel highlights racial profiling against people of African descent’, UN News, 27 February 2017, https://news.un.org/en/story/2017/02/552282-germany-un-rights-panel-highlights-racial-profiling-against-people-african

73 ‘European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection’

74 Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0633

75 ‘European Parliament’s Civil Liberties Committee adopts proposal giving law enforcement authorities and Europol access to Eurodac’, Statewatch News, 19 November 2012, http://database.statewatch.org/article.asp?aid=32044

76 ‘Smart borders: “no sufficient evidence” to justify law enforcement access to proposed Entry/Exit System travel database’, Statewatch News, September 2014, http://database.statewatch.org/article.asp?aid=33953

77 ‘Council of the European Union: Access for law enforcement purposes to the EES’, Statewatch News, October 2015, http://database.statewatch.org/article.asp?aid=35590

78 European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS)’, 16 November 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0731

79 European Union Agency for Fundamental Rights, ‘The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)’, 30 June 2017, p.29, https://fra.europa.eu/sites/default/files/fra_uploads/fra-opinion-02-2017-etias.pdf

statewatch

STATEWATCH.ORG