FIGHTING AGAINST DIGITAL FORTRESS EUROPE:

EUROPEAN DATABASES AND THE POLITICS OF VIOLENT BORDERS

PURPOSE OF THIS ZINE:

Borders remain central to maintaining global structures of power that exist today, where immigration policies become central to the organisation of nation states. There is currently a proliferation of technology within the field of immigration control, much of which is designed to track, identify, detain and deport illegalised migrants. Policy developments such as the European Artificial Intelligence Act, the expansion of biometric migration databases and the use of drones at external borders of Europe, demonstrate the growing importance of technology within security focused, hostile immigration policy. At the same time, 'seamless' airports are under development, where security gates will cease to exist as technology tracks and identifies travellers moving through the airport. This is presented as a vast improvement for 'desirable' travellers, with a focus on cutting down waiting times at airports. But what is the impact of increasingly digital borders for those whose mobility rights are curtailed, for those who are illegalised and excluded, for those from former colonies, or those fleeing persecution, who are denied freedom of movement and subject to scrutiny at every turn?

This zine is part of ongoing research undertaken for the DATAJUSTICE project between 2018 – 2022, and more recently as part of an Economic and Social Research Council (ESRC) research fellowship between 2023 -2024. The questions driving this research focus on the datafied elements of exclusionary asylum and immigration policies in Europe. As well, it asks what impact colonial structures and hierarchies of humanity continue to have on the distribution of mobility rights. The aim of this zine is to demystify complex border technologies, often described as a 'black box'. In doing so, it hopes to further enable community engagement and wider public scrutiny of Digital Fortress Europe.

Fighting Against a Digital Fortress Europe:
European Migration Databases and the Politics of Violent Borders.

**RESEARCHER:
DR PHILIPPA METCALFE.**

BIO:

I am currently an ESRC Postdoctoral Research Fellow. My research explores disparate experiences of datafied and securitised borders, focusing on how both current developments and historical structures impact the lived realities that illegalised travellers and people seeking asylum face in the UK and the EU today.

Prior to this, I completed my PhD as part of the DATA JUSTICE project, based at the Data Justice Lab at Cardiff University, UK. For this, I conducted empirical research in Greece and the UK, exploring how control, power, and violence becomes operationalised within the datafied border and asylum regimes of Europe.

My research demonstrates how new technologies within datafied border and asylum regimes exhibit both exceptional and mundane forms of control and power, where technologies work to simultaneously occlude, invisibilise, and intensify border controls as they become embodied and enacted both at the physical border and across the everyday.

**ARTIST:
RIVER NASH.
BIO:**

River is a carpenter, educator, artist, and designer. Their work on this zine is intended to help make the research within it, accessible to those fighting against the injustice of violent borders, both inside and out of academic settings.
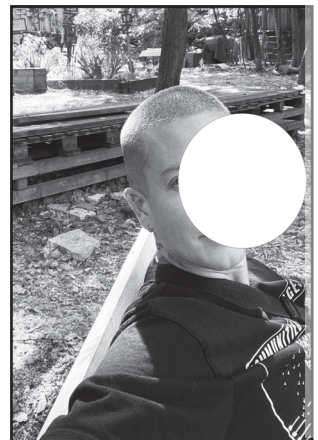
CONTENTS
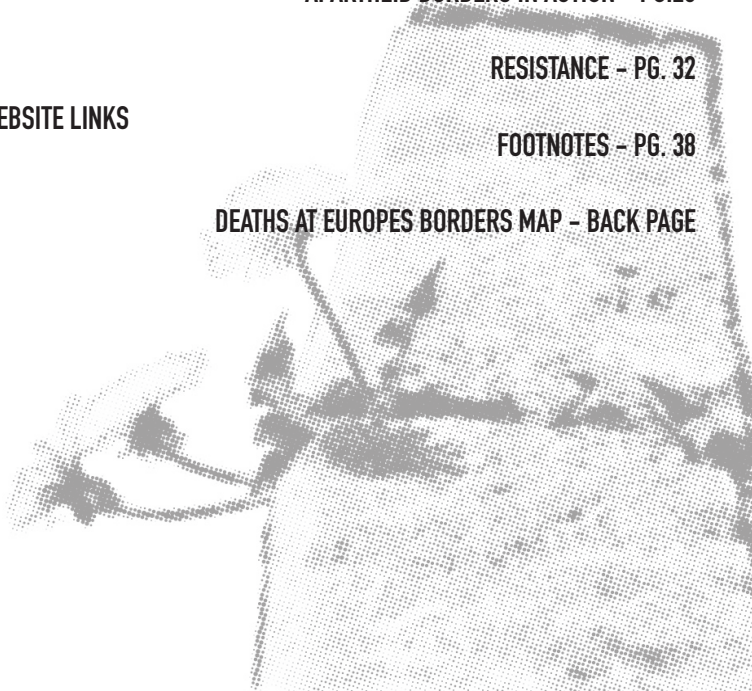
ZINE INTRO

This zine visualises some of the key elements of Digital Fortress Europe: the digital infrastructure of the European border regime. It does so to demystify complex and opaque border technologies. The border regime is made up of a multitude of controls and technologies, from pushbacks at the border, to the use of drones and surveillance to prevent entry to Europe, the biometric identification and categorisation of people after they arrive, violent practices of detention and deportation, wider criminalisation of movement and people on the move, and long waiting times in inadequate accommodation in camps or hotels. These techniques enforce exclusionary and hostile policies that aim to control, prevent, and deter 'undesirable' migration in Europe. Key to increasingly hostile border policy in Europe is the ongoing development of expansive and interoperable migration databases. The EU is pursuing an Interoperability Framework across the fields of borders, policing, asylum and migration. Interoperability here speaks of the ability for digital systems to work together and exchange data across different platforms for the goal of migration control. Importantly, as we shall see, databases have differential impacts on a person depending upon their positionality. Here, borders work as a global apartheid system that dictates who does and does not have free movement. This zine will explore three large-scale migration databases currently in operation across the EU.

CONTROL.PREVENT.DETER / CONTROL.PREVENT.DETER. CONTROL
DETER.CONTROL.PREVENT DETER / CONTROL PREVENT DETER
PREVENT DETER / CONTROL PREVENT.DETER / CONTROL PREVENT
CONTROL.PREVENT.DETER / CONTROL.PREVENT DETER. CONTROL
DETER CONTROL PREVENT.DETER / CONTROL PREVENT DETER
PREVENT DETER CONTROL PREVENT.DETER / CONTROL PREVENT
CONTROL.PREVENT.DETER / CONTROL.PREVENT.DETER. CONTROL
DETER CONTROL PREVENT DETER / CONTROL PREVENT DETER

CONTROL.PR

All 3 databases use biometrics to make individuals legible to states in order to enact border control:

The Schengen Information System (SIS II)

The European Dactyloscopy Database (Eurodac)

The Visa Information System (VIS)

Inspired by the StopLAPD Spying Algorithmic Ecology abolitionist tool, the zine maps out the ideologies, institutions, actors, and impacts of these three databases.

Finally, the zine touches on the imminent expansions of the digital infrastructure as part of the Interoperability Framework and the recently agreed EU Pact of

Migration and Asylum, where surveillance and identification practices look set to become much more widespread, presenting further risks to the welbeing and safety of any person deemed a 'risky' or 'illegal' traveller.

A quick note on terminology:
we often use the term people on the move rather than migrants when referring to people travelling through Europe's borders. This is to centre someone's humanity as opposed to labelling and defining someone as a migrant first and foremost. We have also used the term 'illegalised migrant' rather than 'illegal immigrant'. This recognises illegalisation as a process realised through hostile border policies: **no human is illegal.**

EVENT.DETER//

ARTIST: OKAY, SO WHY DO YOU WANT TO MAKE THIS ZINE?

RESEARCHER: For me, the main point of the zine is to create an accessible means of understanding complex digital border infrastructures. The three main databases we look at (SIS II, VIS and Eurodac) are not new - Eurodac is over 20 years old! But still, there is limited engagement with them: how they work, what impact they have, who profits from them, and how they can be resisted.

Of course, impacted communities know a lot about these systems, but the databases still do not remain at the heart of much political organising despite the huge impacts they have. The result of this has arguably been a huge expansion of digital border controls with little resistance to their development. On a wider level this has meant that the expansion of digital 'solutions' to the ongoing portrayal of migration as a security 'problem' has continued with far too little scrutiny. Of course, that isn't to say there isn't some amazing and dedicated work by campaign groups focused on the expansion of surveillance technologies and identification techniques used for border control. But still, these often remain as a separate movement to much campaigning around racial violence and harmful borders. I think a lot of this could be to do with digital infrastructures seeming invisible, far removed, and overly complex and technological – which takes us back to the point of the zine, to try and address this!

ARTIST: DO PEOPLE FROM THE EU/UK INTERACT WITH THESE SYSTEMS?

RESEARCHER: Yes and no - a lot of it depends if you are a British or European citizen or not, where citizens of these territories generally face much less mobility restrictions and so interact less with migration databases. In the UK, before Brexit anyone who was claiming asylum in the UK would interact with Eurodac at some point – normally when they first arrive and have their fingerprints taken. Ironically, Brexit meant that the UK no longer has access to SIS II or Eurodac, meaning there is less opportunity to track criminalised migrants or try and refuse responsibility for an asylum claim. For SIS II, European and UK nationals can be registered in the database if an alert has been sent out for them to other EU member states. For VIS, only third country nationals applying for a Schengen visa will have to interact with this. As the UK is granted visa free travel to the EU, British citizens do not have to interact with it, the same for other countries which are granted visa free travel, such as the USA, Canada, and Australia. However, when the European Travel Information and Authorisation System (ETIAS) is introduced (which we talk about later in the zine), these travellers will have to enter biometric data in order to enter EU/Schengen territory. I think this shows that techniques which have been 'tested' out on illegalised communities are often later adopted to wider populations once they have become accepted as a legitimate means of control. In this case, we see the widespread adoption of biometric controls.

ARTIST: PEOPLE THAT DON'T HAVE AN ABOLITION-IST MINDSET MIGHT READ THIS AND THINK, 'BUT CRIM-INALS SHOULDNT GET INTO EUROPE' - WHAT WOULD YOU SAY TO THAT?

RESEARCHER: I would say that we should be careful to recognise the power of the state in getting to decide who is criminalised and who is not - and to remember that this can change at any time. I would also ask people to consider, what about wanting to move freely (as white Europeans do) makes someone a criminal? More than this, I would high-light that people on the move only become seen as a criminal due to moving through borders without prior permission. How are people supposed to move legally if there are no legal routes open to them? Does that make them a criminal?

Ultimately, I believe that no one is illegal, and it is the colonial world order and resulting border regimes that nation states impose that are the true crimes to be addressed. Of course, I recognise that not everyone has this mindset, but I hope that by linking together larger ideologies with the harmful impacts on people on the move, this zine goes some way to illuminating that these systems implicitly criminalise racialised and historically excluded communities – this is a feature, and not a bug of the systems.

ARTIST: WHAT MAKES YOU THINK THESE SYSTEMS ARE RACIST? ARE THEY NOT JUST NECESSARY MIGRATION CONTROL, IN THE SAME WAY EUROPEANS CAN'T JUST WORK AND LIVE IN THE USA FOR EXAMPLE?

RESEARCHER: If we take the example of 'random' checks at airports across Europe, and how racialised people with black and brown skin are stopped routinely for 'random' checks: if it is always racialised people that are stopped, it is not random, it is racist. There are many more examples of the ways in which black and brown bodies have historically been, and continue to be, classed as a national security risk.

These experiences have fed into the datasets that lead to racist algorithms and digital infrastructures. If we look at visas for example, the UK used a visa streaming algorithm that categorised people via a traffic light system based on nationality. Countries with previously low recognition rates were flagged as red, often these were former colonial countries and overwhelmingly they were countries where people were not white.

I think at the core of these debates is a recognition of who is granted free movement and who is not. Of course, we are all restricted to some degree by our nationality and passports, but if I want to travel the world I can take a plane, even if I have to apply for visas. What is important is the extent to which our nationalities impact which borders are open to us and the routes of travel we can take to reach our destination. I would not have to risk my life in an overcrowded boat, trying to hide from coast guards who wish to push me back to the country I fled from. Others face this daily. To me, this is inherently racist, cruel, and unfair.

12.

ALGORITHMIC ECOLOGY
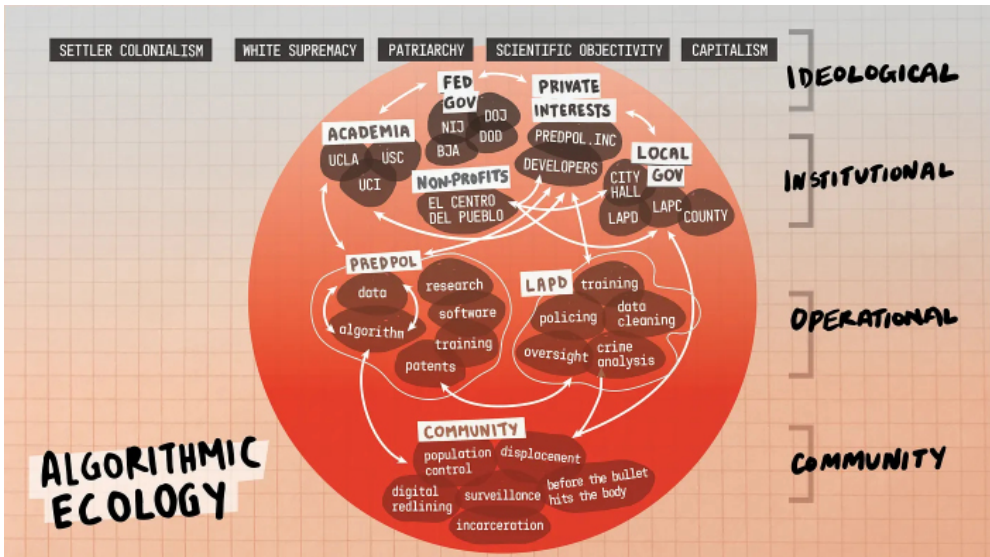
Algorithmic Ecology:

"The Algorithmic Ecology is not just an analytical tool, but a tool for resistance. It is a tool that shows that abolition is both necessary and possible."

This zine takes inspiration from StopLAPD's "Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms". Algorithmic Ecology was used by the Stop LAPD Spying Coalition as a tool to identify the key architects, players, and victims of a predictive policing algorithm called Pred-Pol. PredPol claims to 'predict' crime by using an algorithm to process historical crime data. The algorithm outputs 500x500 square foot geographical boxes or 'hotspots' to direct LAPD officers to patrol areas where crime is supposedly most likely to occur. Rich neighbourhoods are rarely so tenaciously policed. Hence, hyper-policed communities create biased data that feeds back into the algorithms, leading to further heavy policing, perpetuating a vicious cycle of classist and racist oppression under the guise of neutrality. Data-driven policies tend to claim objectivity and lack of bias, but in the case of PredPol, the data is distorted by precluding racism and classism. The Stop LAPD Spying Coalition, along with the Free Radicals activist collective and local community, mapped out the connections between institutions, political actors, and financial interests, arriving at Algorithmic Ecology. The tool identifies four layers: ***ideologies, institutions, operationalisation, communities.*** The intention was to critically examine the actors behind supposedly neutral datasets. *'The Algorithmic Ecology is both a framework and an organizing tool that can be critically applied to any algorithm. This model decentres the algorithm itself, looks at the different actors that shape the algorithm, and illustrates whose interests the algorithm serves, with the ultimate goal of dismantling the actors creating algorithmic harm. The Algorithmic Ecology is also a reminder: We must critically examine what lurks beneath "scientific," data-driven policing, and we must go beyond technology-centered critiques of algorithms and "dirty data."'*

The result of such mapping exercises is not only to visualise complex systems but also to identify actors and spaces for intervention and disruption; with an aim to abolish both the harmful practices and the overarching ideologies themselves. As well, it makes it possible to understand how the harmful impacts on communities are implicit to the design and use of the systems. Whilst not an exact copy of the mapping exercise laid out by the Algorithmic Ecology tool, the diagram below and the next pages seek to demystify complex border technologies, identify the actors and contracted companies, and highlight the human cost of those targeted by migration databases. Through doing so, the zine invites readers to question what should be centred in the fight against harmful (digital) bordering practices. We have adapted the Algorithmic Ecology template and changed 'communties' to the 'impact' to draw attention to the widespread and long lasting impact of border controls on free movement. Through visualisations and mapping exercises, the next pages set out the intricacies, ideologies, and impacts of three of the main EU migration databases.

This text is a summarisation of the article 'The abolitionist Tool For Organizing Against Algorithms' found at: 'https://stoplapdspying.medium.com/the-algorithmic-ecology-an-abolitionist-tool-for-organizing-against-algorithms

DIGITAL FORTRESS EUROPE

INSTITUTIONAL

OPERATIONAL

IMPACT

OVERARCHING IDEOLOGIES

COLONIALITY. WHITE SUPREMACY. TECHNO-SOLUTIONISM AND SCIENTIFIC OBJECTIVITY. RACIAL CAPITALISM.

EU PARLIAMENT
EUROPEAN COMMISSION
EUROPEAN DATA PROTECTION PROGRAMMES
EU COUNCIL   EUROPEAN AND MEMBER AND SCHENGEN STATES   IDEMIA
SOPRA STERIA   ATOS
HP   ACCENTURE   GEMALTO   BULL

FRONTEX   EURODAC   VIS
IMMIGRATION ENFORCEMENT   BORDER GUARDS
VISA OFFICERS   SIS II   POLICE OFFICERS

DEPORTATION   PUSHBACKS   TRAVEL BANS
LACK OF ACCESS TO ASYLUM   DANGEROUS JOURNEYS
CRIMINILISATION   EXPLOITATION   ILL HEALTH
SUICIDE   DETENTION
SEPERATION   EXCLUSION
DEATH

14.

The ideologies guiding the expansion of a digital fortress Europe arguably remain the same across all three databases to be explored. These are identified here and we ask you to consider how each ideology shapes the design, use, and impact of the databases to be explored in this zine. Through recognising how these ideologies shape and perpetuate exclusionary and hostile border controls we see the larger structures of power that need to be challenged beyond the border regime itself. It is these structures that have led to apartheid mobility regimes, which profit and feed upon the subjugation of communities. It is these ideologies which must be challenged if we are to abolish border controls, digital or otherwise.

COLONIALITY:

Colonialism refers to practices of domination, dispossession, occupation, and exploitation of one group over another. These practices were implicit to the formation of European empires and continue to shape global power structures and nation states. Coloniality is a term to reference and recognise the ongoing dominance of a Western-centred capitalist world order.

Within this, the structures of society and states are ordered according to colonial thinking and practices. For example, this impacts which bodies are seen as valuable and which as disposable or unimportant. This then dictates which bodies should be excluded through border controls. Through recognising coloniality as a guiding ideology in (digital) border controls that are hostile towards illegalised and racialised migrants, we can see how the oppression and exclusion of colonised populations and countries has continued
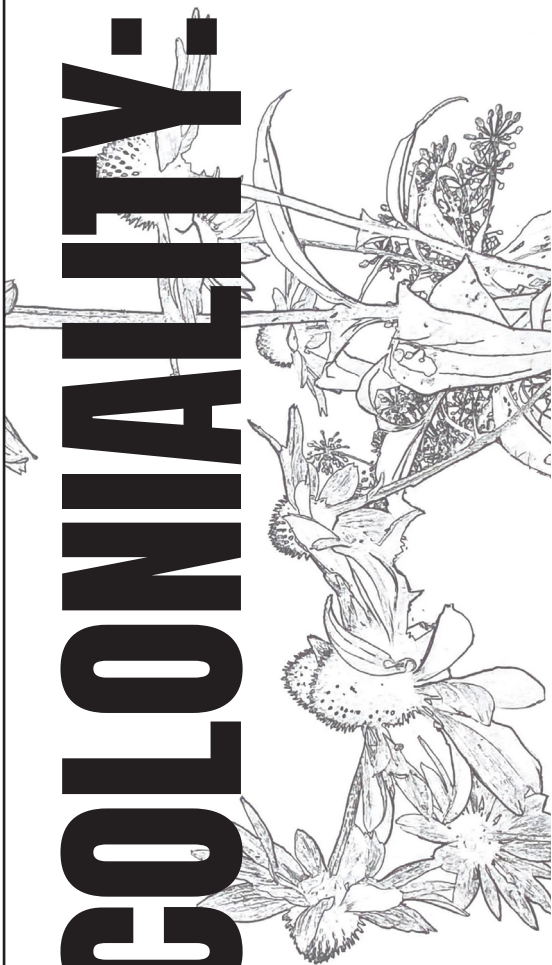
WHITE SUPREMACY:

White supremacy relies upon the hierarchical ordering of race, and the belief that the white race is legitimate in maintaining control over other races.

This ideology shapes much social, economic, and political structures across the world, which operate to further embed differential power according to racialised world orders.

The impact of white supremacy is felt across borders, mobility, policing, and social welfare. As well, it is felt in the every day where racist attacks occur in cities and towns across the world. It rests upon the idea that white lives are more important than others, and their safety must be upheld, even at the cost of harm to non-white bodies.

This is apparent in the ongoing genocide in Gaza where Palestinians are constructed as less than human, or where searches for white billionaires lost at sea in their mega yachts is front page news whereas the almost daily deaths of racialised migrants at Europe's sea borders are invisibilised.
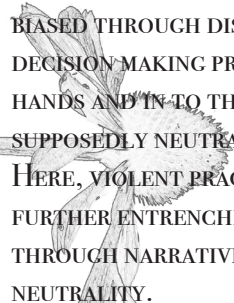
As well, recent white supremacist riots in the UK (2024), where people attacked hotels that housed people seeking asylum, show how these ideologies are very much alive in contemporary societies.

TECHNO-SOLUTIONISM:

This ideology follows the belief that technology heralds the solution to complex and nuanced societal problems. Further to this, it upholds technology as a neutral and objective tool, ignoring the histories and biases built into many technological systems that shape their design, use, and resulting impact.

For example, let's look at predictive policing technologies that are shaped by data on historically racist policing practices. When this data is fed into algorithms used for predictive policing, the technology is far more likely to identify racialised individuals as a criminal threat due to police historically targeting and arresting more black people (this has been shown to be the case across Europe and the USA). However, such solutions are often sold as being less biased through displacing the decision making process out of human hands and in to the hands of supposedly neutral algorithms. Here, violent practices become further entrenched and obscured through narratives of technological neutrality.

RACIAL CAPITALISM:

RACIAL CAPITALISM ASSERTS THAT RACE AND PRACTICES OF RACIALISATION ARE FUNDAMENTAL TO CAPITALISM, WHICH HAS SINCE ITS INCEPTION RELIED UPON THE HIERARCHICAL ORDERING OF PEOPLE AND THE EXTRACTION OF PROFIT AND VALUE FROM RACIALISED BODIES.

ACROSS DIGITAL FORTRESS EUROPE AND BORDER SECURITY INDUSTRIES, WE SEE HOW RACIAL CAPITALISM INFORMS THE EXTRACTION OF PROFIT FROM THE ONGO-ING SUBJUGATION AND EXCLUSION OF RACIALISED MIGRANTS. HERE, LUCRATIVE BORDER 'SOLUTIONS' ARE SOLD AT THE COST OF VIOLENCE ENACTED UPON RACIALISED BODIES.

OTHER EXAMPLES CAN BE SEEN IN THE PRISON-INDUSTRIAL COMPLEX WHERE RACIALISED COMMUNITIES ARE DISPROPORTIONATELY TARGETED AND CRIMINALISED, AND WHERE PROFIT IS TAKEN FROM FINES, BAIL MONEY, AND EXPLOITATION OF PRISON LABOUR.

THE SCHENGEN INFOMATION SYSTEM

The Schengen Information System (SIS) [1] was introduced in 1995. It is now in its second form, referred to as SIS II. The database follows a security narrative and is central to enforcing the surveillance of unwanted persons across the Schengen area whilst also facilitating the free movement of EU citizens. The database provides the basis for cooperation in law enforcement and protection of the external borders across Europe.
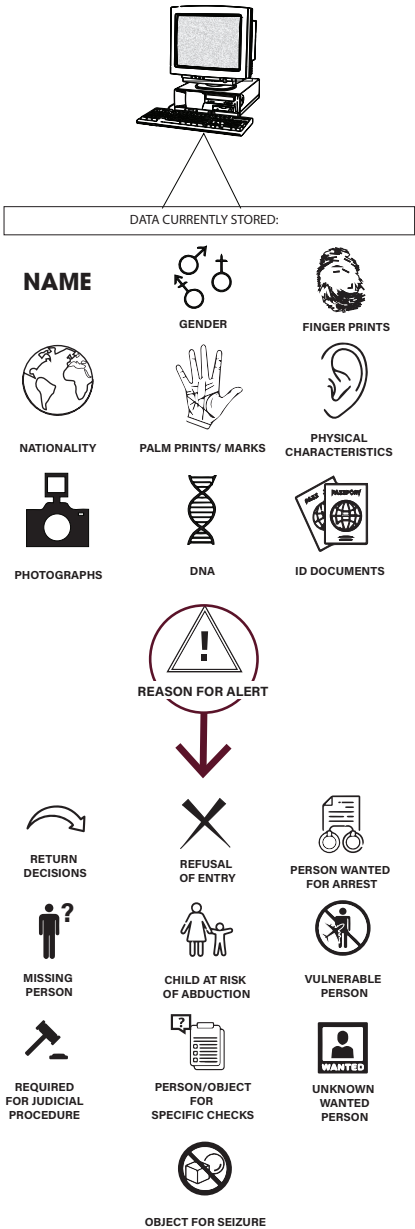
Another database that speaks to law enforcement efforts is the **European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN),** which allows information exchange between member states on Third Country Nationals with criminal convictions in one or more EU states.

SIS II works by allowing states to send out alerts on people who pose a supposed threat to national security, facilitating travel bans on the right to enter or stay on EU territory as well as criminal investigations. When a person crosses a border in Schengen, their details are checked across the database and if an alert is present, they can be denied entry or subject to police controls or even deportation.

SIS II is currently used by 30 countries and operates through a centralised system, as well as coordinating with national systems, providing a communication infrastructure and containing alerts such as missing persons or objects of interest such as documents or firearms. There have been significant changes to SIS II in recent years. The most recent changes

in 2023 saw the expansion of what biometric data is stored, and a stronger focus on deterring illegalised migration.

In 2023 there were 15 billion searches and 91 million alerts on SIS II [2].

DATA CURRENTLY STORED:

NAME

GENDER

FINGER PRINTS

NATIONALITY

PALM PRINTS/ MARKS

PHYSICAL CHARACTERISTICS

PHOTOGRAPHS

DNA

ID DOCUMENTS

REASON FOR ALERT

RETURN DECISIONS

REFUSAL OF ENTRY

PERSON WANTED FOR ARREST

MISSING PERSON

CHILD AT RISK OF ABDUCTION

VULNERABLE PERSON

REQUIRED FOR JUDICIAL PROCEDURE

PERSON/OBJECT FOR SPECIFIC CHECKS

UNKNOWN WANTED PERSON

OBJECT FOR SEIZURE

Data held for:

"as long as is necessary to achieve that specific alert's purpose" [3]
Data should be reviewed between every 1-10 years depending on the type of alert in the database.

Institutions:

Led by eu-LISA, (The European Union Agency for the Operational Management of Large-Scale IT Systems). eu-LISA also works with: the EU Council, the European Commission and the European Parliament, the European Data Protection Supervisor and the European Court of Auditors.

Contracts:

Sopra Steria

Who it impacts/community/outcomes:

It can impact any EU citizen or Third Country National for whom an alert is issued.
It can be used to enforce Schengen travel bans, and has the power to track, identify, detain and deport people.

Example: Dr. Abu Sittah
Dr. Abu Sittah was denied entry to France on May 4th, 2024, when travelling to speak about Gaza at the French Senate [4]. This came after being denied entry to Germany on April 12th to speak at another event about his experience of treating people in Gaza at the Al-Shifa and Al-Ahli hospitals in October and November 2023 during the ongoing genocide. He had committed no crime, only provided medical care in Gaza, and intended to speak about his experiences. The travel ban has since been overturned through legal intervention [5]. However, the example highlights important issues such as: the discretionary power of when SIS alerts are issued; political nature/abuse of SIS alerts; ability to criminalise and exclude unwanted migrations; lack of transparency over the legitimacy and proportionality of alerts.

20.
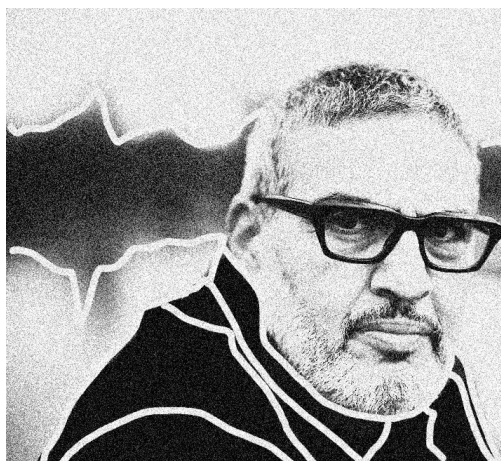
Eurodac [6] is the first Europe wide biometric database, introduced in 2003. It is focused on asylum applications and illegalised mobility. The aim of Eurodac is to prevent multiple asylum applications being made in more than one European Member State. This is part of enforcing the Dublin Regulation. The Dublin Regulation is a mechanism used to assign responsibility for asylum claims between Member States, whereby the first country in which a person was registered should process their asylum claim. This original purpose had arguably since been expanded, exhibiting signs of function creep. For example, allowing policing authorities access to the database for anti-terror and crime activities.

It functions through the collection of fingerprints which are then placed within three categories:

Category 1 stores the fingerprints of applicants for international protection.

Category 2 relates to irregular or unauthorised entry.

Category 3 for persons found illegally present within EU territory.

The database can then be used to search for 'hits' which are used to verify a person's identity and can map out someone's movement across Europe. **As well, these 'hits' are used to determine whether deportation to another Member State** can be justified under the Dublin Regulation.

Changes were made to Eurodac in 2015, where police and law enforcement agencies were given access to the data-

bases. Vast changes are imminent with the voting in of the EU Pact of Migration and Asylum in April 2024, which sees a huge expansion of the use, purpose, and data held within Eurodac [7]. These changes are outlined in the graphics. Notably, the changes will introduce a 4th category to the database: Category 4: people disembarked after a search and rescue operation. Also notable is that Frontex, the European Border and Coast Guard Agency, will have access to Eurodac and be able to transmit data to the system. **In 2023 there were 1,776,914 data transactions through Eurodac [8].**

INFOMATION CURRENTLY STORED:

1ST REGISTERED MEMBER STATE   GENDER   FINGER PRINTS

INFOMATION PROPOSED TO BE STORED AS EURODAC DEVELOPS:

NAME   FACIAL IMAGE   DATE OF BIRTH   ID DOCUMENTS

NATIONALITY   DEPARTURE OR REMOVAL INFORMATION   RELOCATION WITHIN EU   REFERENCE NUMBER

SECURITY CONCERNS   VOLUNTARY RETURNS   APPLICATION FOR INTERNATIONAL PROTECTION
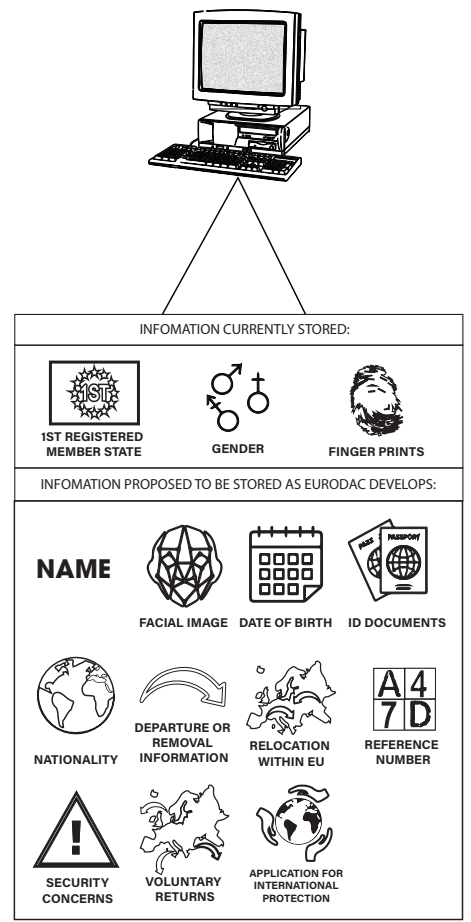
Age Limit
Currently 14, proposed changes will see this lowered to 6 years old

Data Held For
Category 1: 10 years
Category 2: 18 months
Category 3: currently this is not stored, proposed changes to see this increased to 5 years
Proposed category 4-5 years

Institutions
Led by eu-LISA, (The European Union Agency for the Operational Management of Large-Scale IT Systems). eu-LISA also works with: the EU Council, the European Commission and the European Parliament, the European Data Protection Supervisor and the European Court of Auditors.

Contracts
S3B CONSORTIUM (Sopra Steria Benelux (Steria BE), Bull, Gemalto)

Who it impacts/community/outcomes:

Illegalised migrants
People at the borders of Europe and those who have already crossed
People seeking asylum
People on the move

Example/key issue:

Eurodac highlights the violence that people are met with when they first cross into Europe wishing to claim asylum. Here we see hugely unequal power dynamics, where important, life changing data is taken when someone is exhausted and processing a likely danger-ous and traumatic journey. When conducting research and speaking with people who had been subjected to fingerprinting practices for Eurodac, I was told of violence, confusion, lack of information, and an overwhelming lack of choice. For example, Saeed (name has been changed), who passed through Italy and France and was fingerprinted in both coun-tries before reaching the UK, explained his experience in Italy after arriving from a long boat journey.

"[In Italy] I told them that I don't want to give you a fingerprint, but three people came and just took me like that forward, and they took my neck, one of them took my left hand, one took the right hand. And one of them from the behind of my neck put pressure on me they took me in the car, and they told me they were going to send me to prison and three or six months later, we bring you back here and ask you the same question. And again, if your answer is no, we do the same. They put me in car and another officer came to me and told me if you accept to do fingerprints now you don't go to prison. Then I thought that where I am going to in prison with this condition, I should better cooperate with them".
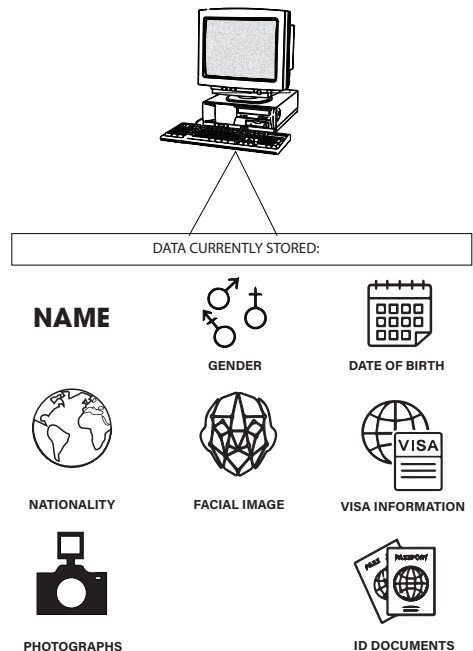
22.

VISA INFORMATION SYSTEM

The Visa Information System (VIS) [9] is a biometric database used since 2011 to enable border guards to verify the identity of a person entering Schengen territory against their visa. VIS enables the sharing of data between EU Member States with consulates in non-EU countries where a person is applying for the visa. This includes sharing information such as previous applications and refusals. Any data entered into VIS is automatically checked across other EU information systems, and it uses an automated profiling system to assess whether a person presents a security or public health 'risk.'

VIS was initially rolled out across a few Northern African countries and is now used for any Schengen consulate in a third country. VIS claims to enable checks and issuance of visas, tackle 'abuse' of visa controls such as 'visa shopping' (making more than one visa application to multiple Schengen states after being refused from one), detect fraudulent documents, protect travellers from identity theft, and enhance security. As well, it is used to aid the implementation of the Dublin Regulation for people seeking asylum through tracing a person's first entry to the EU. In some circumstances, VIS can also be accessed to investigate, prevent, or detect criminal activities. VIS was initially used only for short-stay visas, but in 2021 was expanded to include long-stay visa and residence permits.

Importantly, VIS is used to further externalise the European border, preventing the entry of migrants perceived as 'at risk' of claiming asylum or otherwise overstaying their visa. This places an emphasis on the need to control external borders and

follows the global approach to migration which relies on cooperation with third countries. VIS introduces a stringent and often unattainable screening process before a person reaches the physical borders of Europe. Thus, VIS serves as a filtering mechanism, denying entry to those portrayed as potentially 'illegal.'

DATA CURRENTLY STORED:

NAME

GENDER

DATE OF BIRTH

NATIONALITY

FACIAL IMAGE

VISA INFORMATION

PHOTOGRAPHS

ID DOCUMENTS

Age Limit:

6 years old (12 years for fingerprints)

Institutions

Led by eu-LISA, (The European Union Agency for the Operational Management of Large-Scale IT Systems). eu-LISA also works with: the EU Council, the European Commission and the European Parliament, the European Data Protection Supervisor and the European Court of Auditors.

Contracts

For the maintenance of VIS: BRIDGE3 CONSORTIUM (Accenture NV/SA, Atos Belgium NV/SA, Idemia Identity & Security France SAS).
For developing VIS and the new Entry/Exit System and European Travel Information and Authorisation System: Consortium led by ACCENTURE NV & ATOS BELGIUM NV/SA & IDEMIA IDENTITY & SECURITY FRANCE SAS.

Who it impacts/community/outcomes:

Any third country national migrant who requires a visa to enter the EU Schengen zone. This means racialised migrants are most impacted, as many western imperial nations are permitted visa free travel. VIS thus collects extensive data on people subject to stringent travel rules. It means people's visas are more stringently checked and overstayers flagged. As well, the profiling aspect of VIS means racialised bodies are subject to predictive algorithms that claim to be able to identify people as 'security risks'. Data stored on VIS can lead to future visas being denied.

Example/key issue:

Perhaps the most tangible issue stemming from the use of VIS is the more stringent conditions for obtaining a Schengen visa. Practically, this means that it becomes noticeably harder for people to acquire the needed visa to travel to Europe safely and legally. However, a less well observed impact of stringent visa controls is the economic impact of them. The LAGO Collective [10] researched this under-acknowledged element of visa controls and found that the EU raised €130 million in 2023 alone from visa rejections. This is because the fee for visas is non-refundable, so the EU keeps the money from the cost of the visa application even if the visa is rejected, meaning the cost of visas is pushed onto those who apply for them and the countries they are applying to profit from attempts to obtain visas. LAGO collective also highlights that visa applications from low and middle income countries are more likely to have their visas rejected, with African countries being particularly affected – meaning that it is often those with the least money who pay the highest price for travel.

24.

EU LISA CONTRACT AWARDS 2018-2023 - SIS/EURODAC/VIS
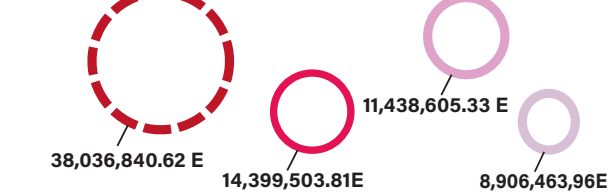
COMPANIES AWARDED:

hp
Atos > (ACCENTURE)

sopra steria

THE S3B CONSORTIUM:
sopra steria
gemalto Bull

BRIDGE 3 CONSORTIUM:
Atos
> (ACCENTURE)   ⟨⟩ (IDEMIA)

> (ACCENTURE)

Atos
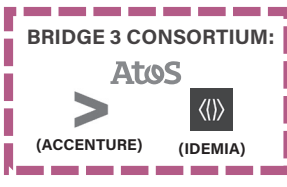
VALUE OF CONTRACT IN EUROS:

2018
2,841,772.11 E
15,599,916.34E
6,963,011.42 E
54,783,467.78 E

2019
34,800,801.08E
4,770,617.61 E
19,413,548.20 E

2020
38,036,840.62 E
14,399,503.81E
11,438,605.33 E
8,906,463,96E

2021
40,000,000 E
18,160,761.63 E
7,382,533.98 E
21,558,923.59 E

2022
21,298,269.74 E
5,672,152.06 E
12,853,069.55 E
40,450,000 E
5,533,406.62 E

2023
8,531,821.91 E
4,795,117.63 E
5,225,316.19 E
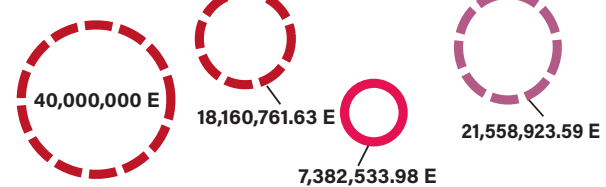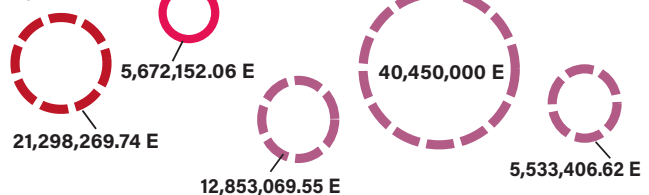
EU LISA CONTRACT - SIS/EURODAC/VIS

TOTAL AWARDED 2018-23:

181,223,528.95 EUROS

154,592,415.74 EUROS

39,188,818.88 EUROS

16,663,921.52 EUROS

8,906,463.96 EUROS

2,841,772.11 EUROS
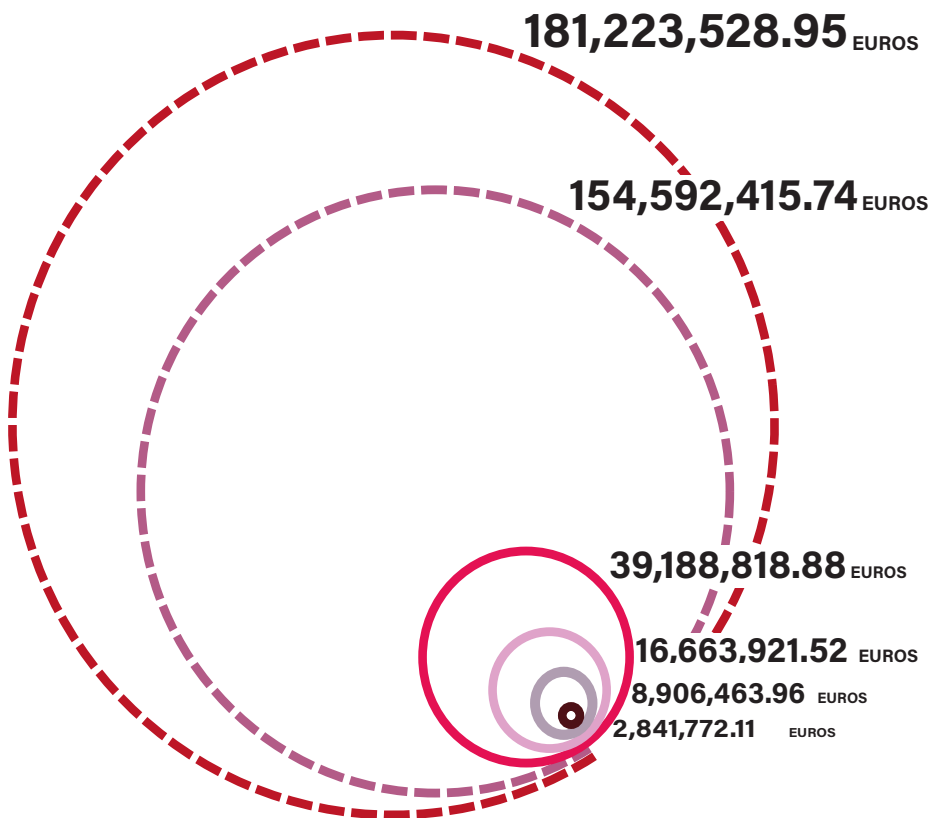
Information for this graphic was taken from eu-LISA's 'Ex Post Publicity' page:
https://www.eulisa.europa.eu/procurements/ex-post-publicity

BIG BORDERS, BIG MONEY

FUTURE DEVELOPMENTS

Future developments to expansive digital migration infrastructures are being developed to reinforce Digital Fortress Europe. Developments to databases include the roll out of these three systems:

ENTRY/EXIT SYSTEM (EES):

The implementation of EES has been repeatedly delayed and is now supposed to come into effect in late 2024 or the first half of 2025. The EES will replace the use of passport stamps in non-EU travellers upon entry to Schengen territory. It will be an automated IT system that tracks and records when and where a Third Country National crosses into EU and Schengen territory, presented as a means of saving time for both travellers and border staff. Details on any previous refusals to Schengen territory will also be recorded in EES.

Stated aims of EES include a more robust system to identify travellers who have not been given permission to enter or stay in the EU, or who have overstayed in EU territory. As well, it aims to prevent the use of fraudulent documents, and facilitate the prevention, detection, and investigation of criminal activities.

EUROPEAN TRAVEL INFORMATION AND AUTHORISATION SYSTEM (ETIAS):

Due to come into force in the first half of 2025 (although the start date has been pushed back many times), ETIAS will store information on travellers who are entitled to visa-free travel in the EU. Based on the electronic system used in the US, travellers will need to enter their details before they travel to request authorisation to enter EU and Schengen territory, details will be attached to a person's travel documents, and will last for three years, or until the document expires (whichever comes first).

The ETIAS website states that the authorisation scheme exists for those who do not pose a security 'risk' to the EU:

"These visitors have been granted visa-free access to the EU and Schengen member countries through virtue of their good track record on security issues and, thus, have not been deemed as a threat to EU security[1]."

THOSE THAT DONT

THOSE THAT HAVE
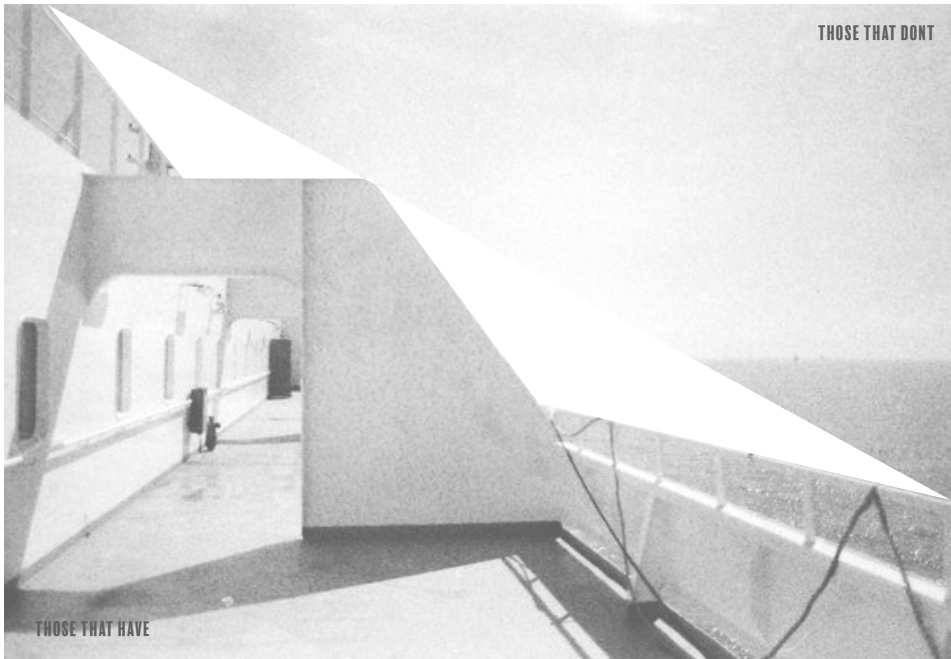
As visa free travel is almost entirely based on nationality, this statement exposes the truth surrounding practices of pre-emptive categorisation of travellers frome some countries as a security 'risk' that we saw in the use of digital visa systems.

COMMON IDENTITY DEPOSITORY (CID):

The CID will create a database that spans across Eurodac, VIS, EES and ETIAS, where data stored in each will be pooled and stored in a single database. This is key to the development of an interoperable and expansive Digital Fortress Europe.

The development of this depository raises concerns, as Statewatch has noted: "Once it comes into use it will be one of the largest biometric databases in the world, with a capacity of at least 300 million records."[2]

Alongside the CID, the development of a Multiple Identity Detector will be used to flag when duplicate data are stored across the interoperable databases, leading to further investigations on the data entered and the person the data relates to.

28.

NUMBER IN MILLIONS

7
6.5
6
5.5
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
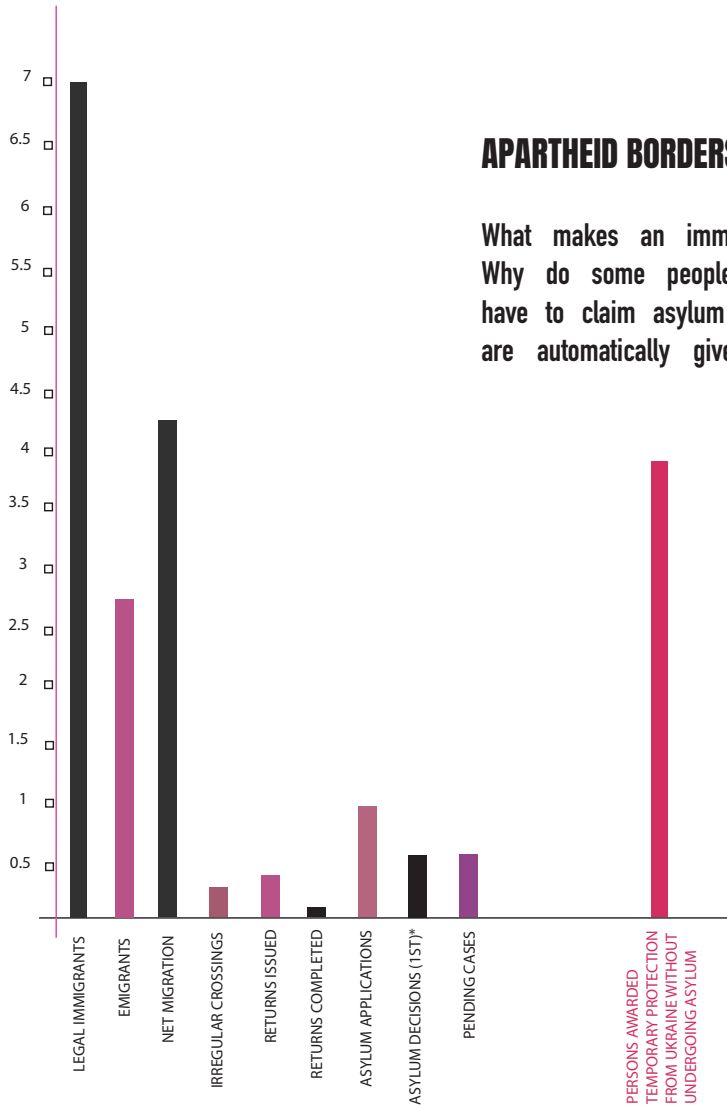
APARTHEID BORDERS IN ACTION.

What makes an immigrant 'legal'? Why do some people fleeing war have to claim asylum whilst others are automatically given protection?

*First instance decision means a decision granted by the respective authority acting as a first instance of the administrative/judicial asylum procedure in the receiving country.

- LEGAL IMMIGRANTS
- EMIGRANTS
- NET MIGRATION
- IRREGULAR CROSSINGS
- RETURNS ISSUED
- RETURNS COMPLETED
- ASYLUM APPLICATIONS
- ASYLUM DECISIONS (1ST)*
- PENDING CASES
- PERSONS AWARDED TEMPORARY PROTECTION FROM UKRAINE WITHOUT UNDERGOING ASYLUM

MIGRATION STATISTICS FOR EU (2022)

FREEDOM OF MOVEMENT & EMPATHY DEPEND ON WHERE YOU COME FROM

Information for this barchart was taken from :

https://english.elpais.com/international/2024-01-11/migrant-deaths-and-irregular-arrivals-reached-a-new-high-in-the-eu-in-2023.html#

https://euaa.europa.eu/latest-asylum-trends-annual-overview-2022

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/statistics-migra-tion-europe_en#seeking-asylum-in-europe

IMPACTS

This list is of course not exhaustive, and the impacts of Digital Fortress Europe and violent borders are far reaching. However, here are some which we have identified as a means of drawing attention to the violence inflicted through Europe's desire to control, prevent, and deter illegalised migration:

EXCLUSION: A key impact of these systems is the exclusion of certain bodies from European territory. This exclusion takes place through the denial of allowing travel into Europe, as well as the refusal to let someone stay. Many of the systems discussed in the zine lead to the exclusion of racialised bodies, which become depicted as 'illegal' and 'risky' migrant bodies, to be controlled and removed from Europe.

CRIMINALISATION: Another key impact of the systems discussed in this zine is the active process of criminalisation of migration and people on the move. This refers to construction of systems that criminalise people through denying them access to legal means of travel, forcing people into illegalised routes or practices (including falsifying documents to obtain a visa). This impacts the way in which people on the move are demonised and seen as criminals.

DETENTION: Being flagged as 'illegal' due to your immigration status by one of the databases discussed in the zine can lead to detention. This is a form of imprisonment based on migration status and means someone's freedom is taken away from them.

DEPORTATION: This refers to the forced, and violent, removal of somebody from a nation state territory. If someone is flagged by Eurodac and found to have a fingerprint in another EU member state, they may face deportation back to that country to have their asylum claim processed.

FORCED INTO TAKING DANGEROUS JOURNEYS: If someone is denied a visa then it ultimately means they cannot travel to Europe by plane or other safe routes. This means that instead, people must take dangerous routes including boarding overcrowded and unseaworthy boats, hiding in trucks, or walking by foot over treacherous ground.

EXPLOITATION: One risk of being unable to gain secure migration status is that someone may be more likely to be forced into exploitative conditions, for example working undocumented means people get paid far less. Also, lack of access to safe travel routes means that people face exploitative rates for travel, such as paying thousands of euros to take a dangerous boat journey to Europe. It is much more expensive to travel illegally than it is to board a plane.

LACK OF ACCESS TO ASYLUM: One impact of Eurodac may be that someone is unable to access asylum in a European member state if they have been flagged as being registered in another EU country. This can lead to deportation, as well as long delays in accessing asylum – which in turn has an impact on the services and support available to someone.

TRAVEL BANS: An impact of SIS II may be having a travel ban placed on someone, where access to European territory is denied and realised through the entering of an alert on SIS II. This means a person may not be able to board a plane or be arrested or face interrogation and deportation once they arrive at a European airport.

SEPARATION: Whether through lacking access to safe travel routes, having a family reunification request denied, or lacking the necessary travel documents to visit friends and family, exclusionary migration databases and wider border regimes result in the separation of loved ones through the denial of free movement.

LACK OF ACCESS TO VITAL SERVICES: The systems discussed in this zine have the ability to criminalise people, as well as make it more difficult to obtain secure immigration status. In turn, this can impact whether or not someone can access basic services. For example, access to free health care or education are often dependent on citizenship or immigration status.

ILL HEALTH: As well as difficulty in accessing healthcare due to insecure immigration status, the impact of exclusionary systems and policies that demonise and ostracise people on the move have profound impacts on physical and mental health. Increased stress, mental health crises, avoiding doctors for fear of being detained are all impacts of Europe's violent borders.

DEATH: As shown on the following fold out map (back page), the most violent impact of Europe's border regime is the deaths of people on the move. Many thousands have lost their lives because of taking dangerous journeys to Europe. Many thousands more have lost their lives after they cross Europe's borders. Reports of deaths in detention centres due to violent treatment or suicide are sadly not uncommon. Long term ill health as a result of stress or lack of access to healthcare also kills. It is vital to remember that these deaths are a direct impact of exclusionary systems.

WE TOO HAVE LIVES TO LIVE

RESISTANCE

There are lots of different forms of resistance to Digital Fortress Europe, from people who experience border violence as well as those in solidarity with them. Some forms target the technology itself, others find non-technological means of resistance. Forms of resistance span from the refusal to succumb to border controls through continuing to move, to legal challenges highlighting the discriminatory and racist elements of datafied controls. Here, we highlight some powerful examples of resisting digitalised controls, however this is of course not exhaustive, with people finding many ways to resist control across the everyday.

BY PEOPLE ON THE MOVE...

One of the most notable means of resistance shown by people on the move in the face of omnipresent and far-reaching digitalised controls is to continue moving despite them. This may look like someone being fingerprinted in Greece and having their data entered into Eurodac but then continuing to move to Germany, despite the risk of deportation. This refusal to play by rules that exist to deny free movement is powerful. Despite the increasingly expansive and violent border controls being introduced across Europe and far beyond, migration continues, and people reclaim the power to decide their own movement.

Another example of resistance by people on the move that has been

widely written about and documented over the years is the practice of burning fingerprints to avoid them being scanned and picked up by Eurodac or other migration databases [13]. This involves physical mutilation of fingerprints as a means of refusing to provide biometric data. Of course, this form of resistance means inflicting harm on your body as an act of defiance and refusal. As such, it demonstrates the depths of border violence implicit to digital controls, where people are pushed to such lengths as a means of avoiding other harmful impacts such as deportation.

As well, Stephan Scheel has documented the ways in which people on the move continue to appropriate mobility in the face of biometric controls. Specifically, he talks about how people appropriate control within biometric visas as a part of VIS through the falsification and manipulation of 'real fake' documents [14]. This might look like procuring a real job contract for a fake job to pass the visa process or borrowing money to demonstrate enough savings and then giving the money back once the visa has been granted. His point is that even in light of biometric controls which make faking a visa more difficult, people on the move continue to find ways around controls and continue to practice their right to mobility.

BY CAMPAIGN GROUPS, ACTIVISTS AND PRACTITIONERS

#ProtectNotSurveil [15] is a coalition of migrant and digital rights groups across Europe who have been active during the AI act legislation process. They draw attention the violent uses of AI toward people on the move in Europe, and campaign around four major issues throughout the legislative process, calling on the EU to: 1) Ban harmful AI practices in the migration context; 2) Regulate all AI high-risk systems in migration; 3) Ensure the AI Act applies to EU's huge migration databases; 4) Make the EU's AI Act an instrument of protection.

Other coalitions against harmful data practices at the border are evident in fight against the use of a visa streaming algorithm in the UK. The civil society group Foxglove, together with the Joint Council for the Welfare of Immigrations (JCWI), underwent a legal challenge to prevent the use of a visa algorithm that sorted visas according to nationality and targeted racialised individuals' visa applications [16]. Shortly before the judicial review was due to take place, in August 2020, the Home Office announced it would stop using the algorithm, meaning it never came under scrutiny in the courts. Despite this, the litigation approach was successful in preventing the ongoing use of the violent algorithm.

Another means of resistance is through making certain practices, such as lobbying or profiteering, visible. Research groups including Statewatch, TNI, Corporate Watch, and Privacy International have been central to ongoing documentation efforts, exposing the role of private actors in designing and implementing digital and security focused border controls, naming large technology and arms companies that lie at the heart of border controls in Europe. This provides invaluable insight into what actors could be targeted for public pressure or boycott movements.

34.

As well, practitioners that are forced to use digital systems designed to share information and data taken from migrants have a long history of resisting their use. One notable example in the UK is the Docs not Cops, Patients not Passports, and Migrants Organise campaign groups. These groups are working to end racist practices of data sharing as part of charging practices in the NHS.

These practices set out by the Home Office mean that the NHS employs Overseas Visitor Managers to check the 'chargeability' of a patient through sharing their data with the Home Office to check immigration status. In reality this means Home Office records are kept up to date.

It has been documented that this has led to widespread fear from people with insecure immigration status, who come to fear that interacting with healthcare could lead to being identified for immigration controls, including immigration raids, detention, and deportation [17]. One way in which the groups resist this is through raising awareness amongst clinicians and drawing attention to these harmful practices which take place hidden behind computer screens and automated data sharing practices. As well, the groups campign to challenge and change government policy on this issue. Similar efforts have been shown by NHS staff in their protest against the inclusion of Palantir, a large technology company, in NHS contracts in light of Palantir's on going provision of military and surveillance technology to the Israeli government that is used to oppress and harm Palestinians.

See below for some key reports on this:

HTTPS://WWW.STATEWATCH.ORG/PUBLICATIONS/REPORTS-AND-BOOKS/AT-WHAT-COST-FUNDING-THE-EU-S-SECURITY-DEFENCE-AND-BORDER-POLICIES-2021-2027/

HTTPS://WWW.STATEWATCH.ORG/PUBLICATIONS/REPORTS-AND-BOOKS/EUROPE-S-TECHNO-BORDERS/

HTTPS://WWW.STATEWATCH.ORG/PUBLICATIONS/REPORTS-AND-BOOKS/TELLING-THE-STORY-OF-EU-BORDER-MILITARIZATION/

HTTPS://CORPORATEWATCH.ORG/PRODUCT/THE-UK-BORDER-REGIME/

HTTPS://WWW.TNI.ORG/ES/PUBLICACIÓN/EL-NEGOCIO-DE-CONSTRUIR-MUROS?TRANSLATION=EN

HTTPS://WWW.OHCHR.ORG/SITES/DEFAULT/FILES/DOCUMENTS/ISSUES/MERCENARIES/WG/IMMIGRA-TIONANDBORDER/LEMBERG-PEDERSEN-RUBNERHANSEN-SUBMISSION.PDF

HTTPS://ORCA.CARDIFF.AC.UK/ID/EPRINT/162104/1/RISKING-LIVES-REPORT.PDF

Links to websites mentioned throughout the zine and other useful resources:

PATIENTS NOT PASSPORTS:HTTPS://WWW.PATIENTSNOTPASSPORTS.CO.UK
DOCSNOTCOPS HTTP://WWW.DOCSNOTCOPS.CO.UK
MIGRANTS ORGANISE HTTPS://WWW.MIGRANTSORGANISE.ORG
EUROPEAN DIGITAL RIGHTS (EDRI) HTTPS://EDRI.ORG
ACCESS NOW HTTPS://WWW.ACCESSNOW.ORG/ARTIFICIAL-INTELLIGENCE/
ALGORITHM WATCH HTTPS://ALGORITHMWATCH.ORG/EN/
AMNESTY TECH HTTPS://WWW.AMNESTY.ORG/EN/TECH/
PROTECT NOT SURVEIL HTTPS://PROTECTNOTSURVEIL.EU/#ABOUT
STATEWATCH HTTPS://WWW.STATEWATCH.ORG
PRIVACY INTERNATIONAL HTTPS://PRIVACYINTERNATIONAL.ORG
FOXGLOVE HTTPS://WWW.FOXGLOVE.ORG.UK
JUSTICE, EQUITY AND TECHNOLOGY TABLE HTTPS://WWW2.LSE.AC.UK/JUSTICE-EQUITY-TECHNOLOGY
EUROMED RIGHTS HTTPS://EUROMEDRIGHTS.ORG/

ABOLISHING DIGITAL FORTRESS EUROPE

THROUGH MAKING VISIBLE THE IDEOLOGIES, COMPLEX DATA INFRASTRUCTURES, AND IMPACTS OF AN EXPANSIVE DIGITAL BORDER REGIME IN EUROPE, WE HOPE THAT IT BECOMES CLEARER HOW THESE SYSTEMS WORK.

MIGRATION IS NOT A CRIME. MIGRATION IS NOT

AS WELL, WE HOPE IT INSPIRES ACTION THROUGH SHEDDING LIGHT ON WHO IT MIGHT BE HELPFUL TO TARGET IN THE FIGHT AGAINST VIOLENT (DIGITAL) BORDERS, WHERE KEY ACTORS — FROM EU INSTITUTIONS TO PRIVATE COMPANIES — PLAY A KEY ROLE IN THE DESIGN AND IMPLEMENTATION OF DATABASES.

OT A CRIME. MIGRATION IS NOT A CRIME. MIGRATION IS NOT A

38.
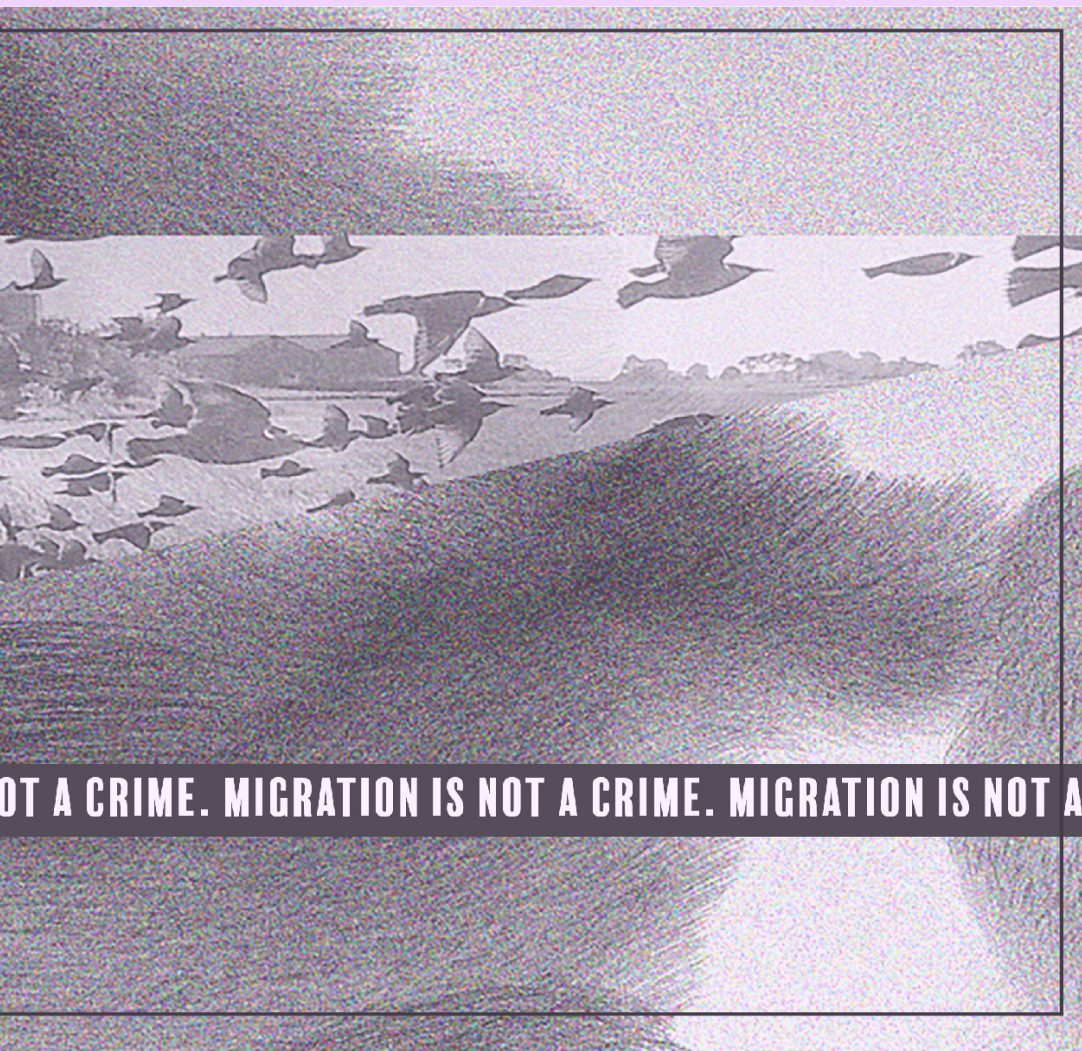
FOOTNOTES

1. https://www.edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en

2. https://www.eulisa.europa.eu/Publications/Reports/SIS%202023%20Annual%20Statistics%20-%20 Report.pdf

3. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/ questions-and-answers_en

4. https://www.middleeasteye.net/news/hrw-called-germany-explain-ban-palestinian-surgeon-ghas-san-abu-sittah-europe

5. https://www.middleeastmonitor.com/20240515

6. https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migra-tion-glossary/glossary/eurodac_en

7. https://picum.org/blog/the-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance

8. https://www.eulisa.europa.eu/Publications/Reports/Eurodac%202023%20Statistics%20Factsheet.pdf

9. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/visa-information-system_en

10. https://www.lagocollective.org/material/f/visas/rejected-by-gdp/, see also https://euobserver.com/ eu-and-the-world/ar1aabb08b

11. https://etias.com

12. https://www.statewatch.org/eu-agencies-and-interoperable-databases

13. Glouftsios, G., & Casaglia, A. (2023). Epidermal politics: Control, violence anD dissent at the biometric border. Environment and Planning C: Politics and Space, 41(3), 567-582. https://doi. org/10.1177/23996544221144872

14. Scheel, S. (2017). Real fake? Appropriating mobility via Schengen visa in thE context of biometric border controls. Journal of Ethnic and Migration Studies, 44(16), 2747–2763. https://doi.org/10.1080/ 1369183X.2017.1401513

15. https://protectnotsurveil.eu

16. https://www.foxglo

17. https://neweconomics.org/uploads/files/Patients-Not-Passports-Migrants-Access-to-Healthcare-During-

Acknowledgments and Thanks

I dedicate the zine to the people impacted and excluded by Digital Fortress Europe and the wider European border regime. For those who struggle against it every day and those who lost their lives at its hands: we will continue to stand with you and fight for free movement for all.