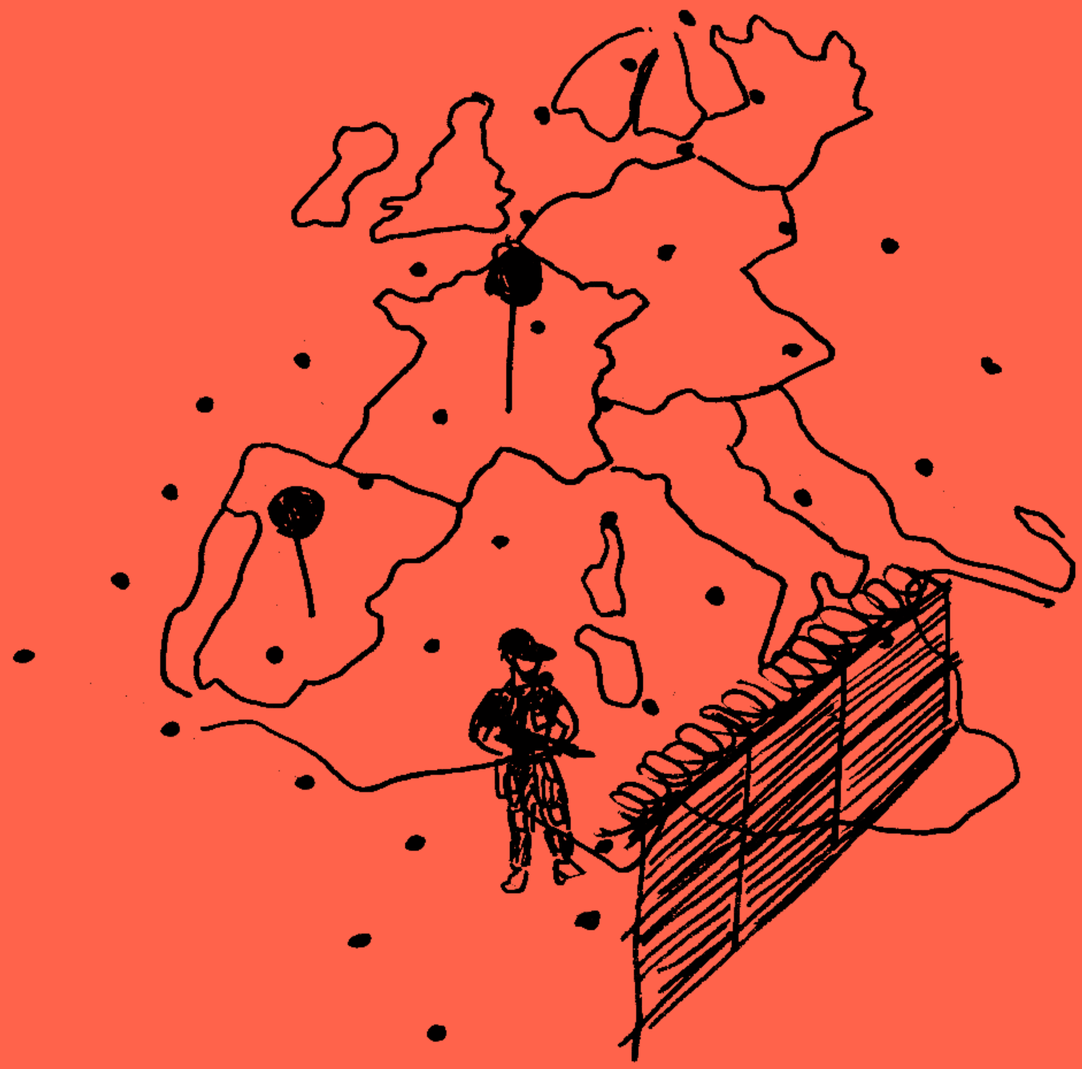
DIGITAL POLICING HARMS

This part of the toolkit will explore different types of digital policing tech, and real examples from organisers of harm they cause, including some efforts to resist against them. It will be split into two broad themes, the digital policing of people, and place. We do this, recognising the two overlap, but to offer context to how the technology is deployed.



DIGITAL POLICING of PEOPLE

In this section, we are exploring : *Data Privacy* **and** *Tracking, Biometric Technology, Ethnic Profiling, Databases* **and** *Data Sets*, **how people are** *digitally policed* **while** *on the move*, **and how** *digital policing* **takes place across** *welfare* **and** *public services*.

(PERSONAL/CONSUMER) DATA PRIVACY AND TRACKING

Privacy is a fundamental human right, and this includes a personal ability to self determine when, where, and how personal or collective information is shared or disclosed, also online. Data Tracking is where software tracks, collects, organises, and analyses user activity through apps, websites, or even offline usage. The tracking is mostly understood to result in targeted advertising but can also be used for specific and targeted surveillance.

In the EU, The General Data Protection Regulation (GDPR) aims to regulate how personal data are collected, categorised, classified, shared etc. in other words - processed.

In its article 4 (1) it defines personal data as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

The GDPR creates exemptions to the protection it guarantees, notably in matter relating to criminal law or what is named "substantial public interest".

The Law Enforcement Directive (LED) 2016/680 foresees a different sets of rules concerning the processing of personal data by law enforcement authorities to "prevent, investigate, detect or prosecute criminal offence". Those two legislative texts restrict the enjoyment to the right to privacy in cases falling under criminal law and the vaguer notion of "security threats".

"Big Data, Big Tech, and relationship/contract/ distribution to governments and state agencies, combined with the power and resource a governmental service has, facilitates the ability for wide impact and international cooperative Global Policing. Tech developed in Europe is being used in the US, and vice versa, around the world. Databases developed by Lexus Nexus in the UK is being used by US ICE. Big Tech equals World Wide policing."

Sejal Zota and Laura Rivera,
Just Futures Law
2023

In 2022, the “Policing in a Digital Age” conference **highlighted** that the Council of Europe launched a new network to “strengthen technological cooperation between the police forces of member states” to enable “knowledge sharing” and participation in “increased cooperation” (Strasbourg, 2022). Governments and policing and enforcement agencies believe that “embracing innovative technologies” is key to future proofing their work for years to come (Richardson, 2022).

Those declarations participate to the myth that because machines can do some operations faster than humans they are more efficient. But in reality, those technologies while widening the scope of surveillance are always reliant on a human decision in the end. There is always a human involved making the decisions.

They create a competition between what is public interest, our safety and our collective and personal right to privacy. But often our collective privacy is in reality key to our safety- when we protest, when we are part of a group that has been historically discriminated and will face the harshest consequences when organising against injustices, when we are living in neighbourhood that are over-surveilled etc. Protecting our personal data in those circumstances and making sure we have ownership of how they are used is key to our safety and is in the public interest.

What we see is that our data collected by private companies can be used for policing purposes- and that rules that apply in Europe do not protect our information in the U.S. for example.

BIOMETRICS

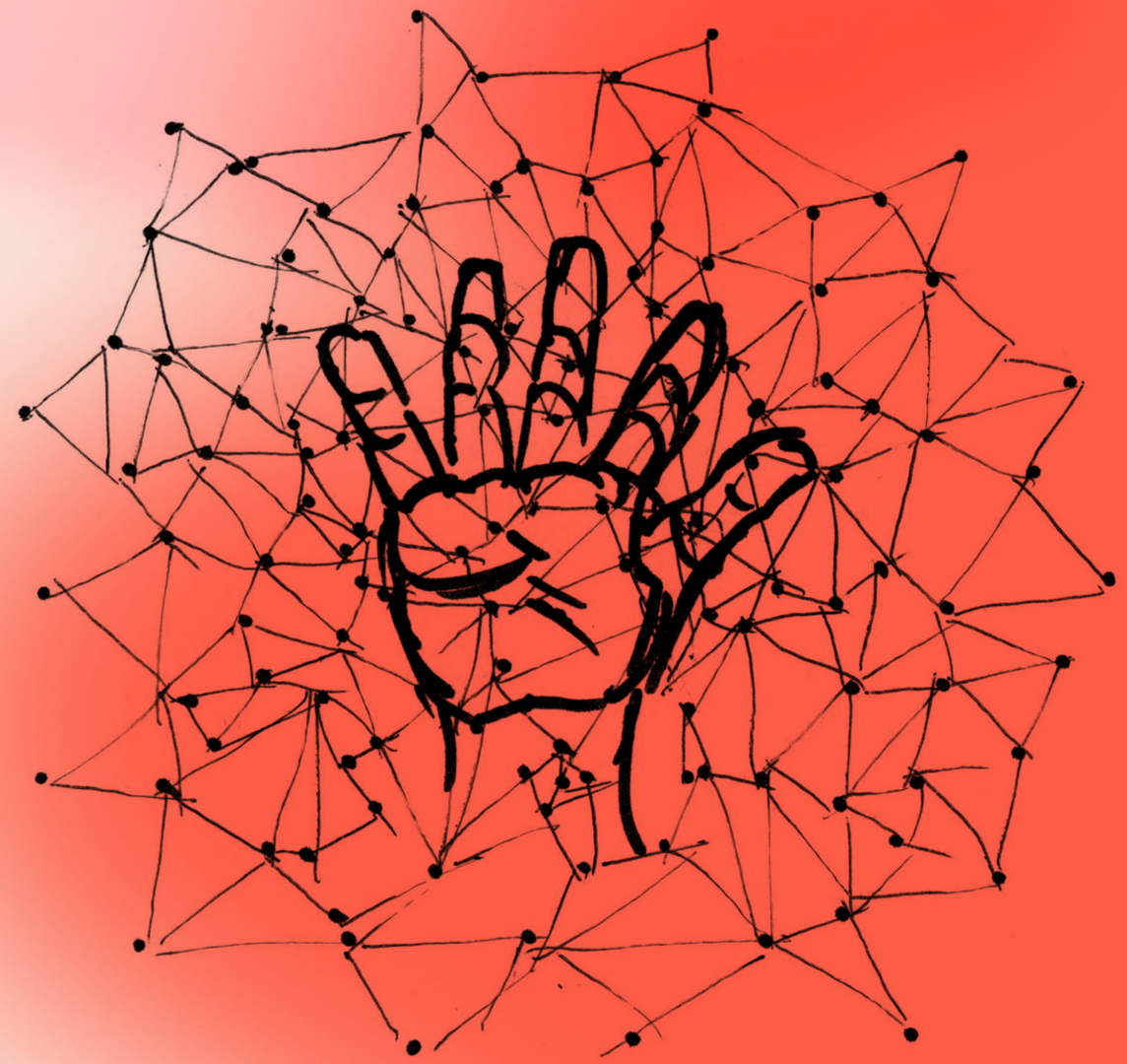
Biometric Data is used to identify and mark a person using recognisable, verifiable, and unique personal data.

Fingerprints, DNA, or the eye (iris/retina) are types of biometric data and are used to verify people's identity. Development in technologies has meant that they are now able to also use behavioural data as biometrics, this includes voice recognition, signature dynamics, and even sounds of footsteps.

The practise of biometrics was used during transatlantic slavery, through the practice of branding the bodies of enslaved people (DFF, 2022). In the current times, the most consistent use of biometrics is in deceased body identification, by police during arrests, across criminal (in)justice systems as criminal evidence, and in border and migration enforcement (Thales, 2023).

Much of this personal data is collected to enable a person to access a service, travel, authenticate themself as required by relevant laws, but little information is given around consent, use, or how it will be stored or protected. Human rights group, raise regular concerns and challenges to agencies, governments and private companies about the scale of the data collected, as well as how it is stored, used and shared (Skelton, 2023).

Biometrics technology is a key part of the enforcement of borders and tracking people on the move. Facial recognition software, and fingerprinting is becoming standard at airports, and now we are seeing personal hand held devices to be used by officers. These devices are often linked not only to national databases, but international ones too. The border control agents work are supported by the tech to identify people on the basis of "risk profiles." Systems storing and processing the biometric data is often built around profiling and algorithms programmed around stereotypes of ethnicities and nationality which results in ethnic profiling, unnecessarily, and intensifies agencies ability to discriminate, criminalise, and harm (Statewatch, 2022).



ETHNIC PROFILING

"On a continent where white supremacy runs deep but is hardly acknowledged, control by the State has structurally included a racialised control. From the control of the colonial subject, to the criminalised 'second-generation' immigrant, the history of policing in Europe is fraught with examples of the criminalisation and targeting of racialised communities"

Esra Ozkan & Sanne Stevens,
JET Table
2021

Ethnic profiling is embedded into the structures of surveillance technology, it captures and triggers based on specific features, such as beards, but also based off skin tone. Ethnic profiling happens at street level policing by officers and through digital policing technology.

To ethnically profile is to create criteria in relation to skin colour, presumed ethnicity, nationality, or religion, assessing these characteristics as risky or potential threat, to be monitored, investigated, assessed or challenged.

Ethnic profiling often takes place through indirect means- legal forms of dog whistling.

For example, in many European States the notion of "terrorist" has been intertwined with racial characteristics, the increase of counter-terrorism has led not only to an increase in criminalisation of racialised communities but also in shrinking of the scope protection of fundamental rights linked to freedom of expression all over Europe. In this, the use of digital technologies play an important role- it is often on the ground of counter, terrorism policies that wide-sharing of information between different law enforcement agencies are allowed, exceptions to data protection in the realm of migration are put in place, former illegal practices by the police are legalised.

In Italy, the ethnic profiling of Roma people and their nomadic culture as inherently criminal, come from underpinning racist views. Building on the historic racism around Roma people in Italy, Roma people are further criminalised and punished through assertions that Roma nomadic culture enables and facilitates criminal planning and enterprise. This has led to social policy "security measures" in digital policing to be built around these stereotypes and led to prolific surveillance and policing of Roma communities (Colacicchi, 2008).

The same treatment of Roma people is seen in Greece, with surveillance and criminalisation of Roma people happening through municipal policing and border enforcement, where migration for people from Roma communities has in effect been criminalised (Eleftherios Chelioudakis, Homo Digitalis, 2023).

DATABASES AND DATA SETS

> "This practice [of the banning letters] was clearly race discrimination - with people from Black and ethnic minority backgrounds more likely to be targeted. The practice was entirely opaque, unfair, and therefore unlawful, and there was no legal justification for sending these banning letters."

Louise Whitefield,
Liberty
2023

The use of digital policing in "gangs" policing is a perfect example of how young racialised people are harmed and criminalised.

80% of people on the Metropolitan Police's (London, UK) Gangs Matrix, a central database managed by the police force to track people who have been deemed as associated, part of, or at risk of becoming a member of a "gang" are aged between 12-24, 78% are Black, 75% have been victims of crime and 35% have never committed an offence (Williams, 2016).

This database exists without a specific legal definition of what constitutes what a "gang" or "gang member" is. The statistics do evidence however that racism plays a key part in the markers used to identify people specifically that being Black, and being Black and young are indeed flags used. This is not only seen in London, but is mirrored in other areas of the UK such as in Manchester where a similar patterns are found. Demonstrating real time examples of systemic racism embedded into digital policing.

Because of its lack of real definition but moreover link to its cultural highly racialised connotation and history, 'Gangs' policing can be seen as a racist tool of Policing (Ana Muñiz 2022, Stuart Hall, 1978).

In Manchester the police utilises a database and a flagging system to identify people around specific markers. This use of databases have led to many people receiving letters from the local law enforcement authority banning them from the local Caribbean carnival since 2006 for being classified as "a member of a street gang", "affiliated to a street gang", "perceived by others to be associated to a street gang", "involved in criminal activity", "arrested at [the Carnival] 2019/2020/2021", or "involved or linked to Serious Youth Violence' with 91% of bans issued to people with non-white ethnicities and Black people 8 times more likely to receive a ban (Lothian-McLean, 2022). Following action and legal challenge from racial justice youth organisation Kids of Colour and legal firm Liberty, in 2023 the letters were not sent that year.

Data Set

Data is information which is collected and stored for later use. A Data Set is the collation of information (data) which can be grouped together based on commonalities.

A Data Set can hold a wide range of people's personal data including ethnicities, nationalities, physical descriptions, and/or postcodes. This information can be accessed individually but can also be manipulated to be sorted or filtered based on commonalities. Common-

ly used in census data (Census, 2023), or in immigration to monitor and track people's movements (Cangiano, 2010). The manipulation of data allows analytics to identify trends and draw conclusions for ongoing monitoring or action based on specific criteria such as "risky" commonalities (TechTarget, 2023).

Database

When data has been organised into a system that can be controlled and managed by a management system a database has been created (Orcale, 2023).

In policing, databases are used to record, track, monitor and surveil people. They are often themed to categorizations such as people "convicted of a crime", "perceived to be a part of a gang" or may relate to a person's citizenship status. Databases allow for checks to be made which may result in action against people included action based on "perceived risks" (Williams, 2023, commonly used in gangs policing such as the London Metropolitan Police Gangs Matrix (Cresto-Dina, 2023). There are huge concerns around the partnership between private companies and the state around the security of data and the lawfulness in which data is obtained, shared and protected (Ye, 2021).

Databases operate within Public Services

In recent years there has been increased privatisation (Spricker, 2009) of the services provided by the State to individuals residing on its territory in matter of education, housing, health, welfare etc (Dan McQuillan, 2022). This has resulted in the deployment of technologies to participate in assessing the risk of potential fraud, this is especially evident around welfare benefits (Lighthouse Reports, 2023). **Far from creating new oppressive patterns,** the technologies merely work as tools of oppressive policies and often reveal how the policing dimensions of public services are intertwined with race, gender, class, disability and nationality.

"For young people databases allow young people's data to be shared across housing, health, education, social services and criminal (in) justice systems, often without their or legal guardians knowledge or consent. And this is how they are able to be monitored, tracked, policed , criminalised, and ultimately punished"

Griff Ferris,
Fair Trials

In Bristol (UK) the local authority work in partnership with policing and statutory agencies such as social services and health to obtain and share data about children and families. **Over 200,000 families are listed on the the "Think Family" database.** It has been piloted in 4 schools and is now on offer to be rolled out, free of charge, across 130 schools in Bristol to enable "timely by crucial" data sharing and accessible to police, from educators, and social services. Many educators and social workers are unaware of the consequence of "recording notes" but **this information will be accessed by the police without barriers, and results in police contact (Bristol Gov, 2023) and ultimately criminalisation.**

In Greater Manchester (UK) the newly launched **"PIED" (Prevention, Intervention, Engagement, Diversion) Project is a partnership between Greater Manchester Police, the Greater Manchester Violence Reduction Unit, the local authority, and wider multi agency groups.** PIED aims to track and identify young people for "interventions" and sees 274 young people discussed at weekly meetings, where information is shared with police and the other agencies. **Rooted in a data-driven approach, the database is also used to identify schools that should have school-based police officers allocated to them,** identify young people who live in so called "high crime areas" and are related/ associated with adults who have offended in the past (LGA, 2023).

WELFARE

In the Netherlands, “racial and ethnic discrimination was central to the design of an algorithmic system introduced in 2013” which was created to identify incorrect applications for child benefits and fraud. The so called “robot debt” used non-Dutch nationality as an indicator, as well as foreign sounding names. Flagged families had benefits suspended, were subject to investigation and benefits recovery, which resulted in significant financial precarity with some losing homes through eviction. The stress and mental health issues it caused led to serious relationship breakdowns, children having to leave families and divorce.

Patrick Williams,
2023

CASE STUDY

The childcare benefit scandal in The Netherlands

“In the childcare benefit scandal, in the Netherlands – a risk assessment algorithm used to assess so called “at-risk profiles” led to families in a precarious situations being penalised after being flagged and being demanded to reimbursed tens of thousands of euros. The risk assessment was based on highly discriminatory understanding of who is a risk profile, where the flags or triggers were based on ethnicity, names, and religion, where people who have made donations to mosques have been targeted” ■ Nawal Mustafa, PILP.

CASE STUDY: ROTTERDAM

Discriminatory algorithm in welfare system in The Netherlands

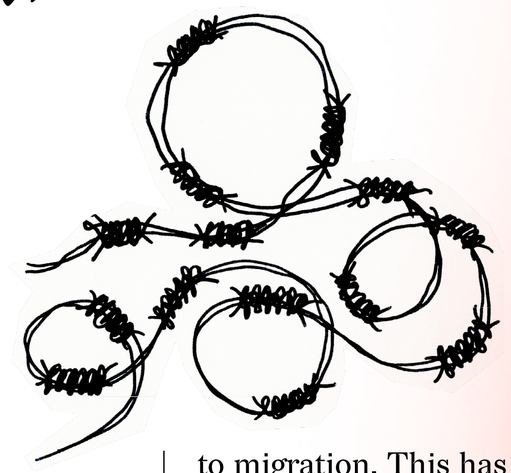
"The risks scoring system we (Lighthouse Report) took apart is a machine learning model deployed by Rotterdam, a major shipping hub and the Netherlands' second largest city. Every year, Rotterdam carries out investigations on some of the city's 30,000 welfare recipients. Since 2017, the city has used a machine learning model – built with the help of multinational Accenture – to flag welfare recipients who may be engaged in "illegal" behaviour i.e. cheating the welfare system. In mid-2021, Rotterdam decided to put the risk scoring system "on-hold" while working to update it. Rotterdam's fraud prediction system processes 315 inputs, including age, gender, language skills, neighbourhood, marital status, and a range of subjective case worker assessments, to generate a risk score between 0 and 1.

Between 2017 and 2021, officials used the risk scores generated by the model to rank every benefit recipient in the city on a list, with those ranked in the top 10 percent referred for investigation. While the exact number varied from year to year, on average, the top 1,000 "riskiest" recipients were selected for investigation. The system relies on the broad legal leeway authorities in the Netherlands are granted in the name of fighting welfare fraud, including the ability to process and profile welfare recipients based on sensitive characteristics that would otherwise be protected (...).

The findings are stark. The suspicion machine passes harsher judgement on: parents, young people, women, people with roommates, people who do not have enough money and people with substance abuse issues. Some of the variables that increase a person's risk score are totally beyond their control: their age and gender for example. Others are fundamental to why people need social welfare in the first place: they face financial problems, they struggle with drug addiction, they cannot afford the rent to live independently. And most problematically, some seem to ethnically profile people based on the languages they speak or their ability to speak Dutch, which is widely considered a proxy for ethnicity."

■ Suspicion Machine, Lighthouse report, 2023.

PEOPLE ON THE MOVE



Digital policing is at its highest when concerning people on the move.

From before people reach EU external borders to long after they have entered one of the member states territory, digital use are used to heightened surveillance and control.

The EU has started explicitly conditioning development money. For countries to receive the money, they have to support the EU in its politics in regard to migration. This has a digital policing component. In the EU emergency trust fund for Africa for example "EUR 11.5 million (are) allocated to Niger for the provision of surveillance drones, surveillance cameras, surveillance software, a wiretapping centre, and an international mobile subscriber identity (IMSI) catcher, an intrusive piece of technology that can be used to locate and track mobile phones by simulating to be a mobile phone tower." Another project supported is a "EUR 28 million programme to develop a universal nationwide biometric ID system in Senegal by funding a central biometric identity database, the enrolment of citizens, and the interior ministry in charge of the system, implemented by the French and Belgian cooperation agencies." ■ Euromed 2023.

"In Schipol Airport the profile of 'Nigerian Smuggler' according to the data was 'Black man, well dressed, walking fast, in the airport'. There were two men who fit this description who were repeatedly stopped by Dutch border enforcement. They spoke out about it and linked with PILP, Clt Alt, Delete, and Amnesty and built a case against the Dutch border police about the use of ethnicity in a risk profile. Initially the case was lost, but this created public outcry, as it mean that only people categorised as white were seen as Dutch. The decision was overturned in appeal, and now the border policing cannot use the criteria of race"

Nawal Mustafa,
PILP
2023

“Homo Digitalis are working hard to build resistance work around the use of new technologies, which enhance criminalisation of the Roma identity in Greece currently in a phase of building relationships, and finding accessible language and translations to reach people who are being policed for being Roma. It is important to us to ensure that lived experience is centred and guides resistance work”

Eleftherios Chelioudakis,
Homo Digitalis

“Homodigitalis is increasingly concerned about how immigration officials are seizing people’s personal tech devices from them when they reach the country under the guise of it being pertinent to identify smuggling rings. Now we need to understand more about the ‘phone scrapping’ which is happening. How the enforcement agencies are obtaining the data and what they are using it for. We are exploring the options of fighting this on a political level but also with the telecom providers themselves”

Alyna Smith,
PICUM
2023

“There are so many contexts of how and where technology is used in the policing of migrants that it is hard to say which is the worst. Things are often so hidden, or at least not obvious that the tech is being used, but we know in some way that it is often present. There’s surveillance at borders - infrared cameras, drones, object detection — different kinds of tech, which raise different types of concerns, but we know that they frequently inform on the ground decision-making”

The use of digital technologies is highly present at external borders of the EU with multiple technologies having been deployed and tested over the years such a sound walls projecting unbearable noise at the greek- turkish borders, coupled with cameras, night vision and multiple sensors, so called “lie detectors” and “emotional AI” based on pseudo-science pretending to detect false testimonies, databases collecting fingerprints, facial features, name, date of birth, country of origin in refugee camps, tracking of entry and leave of the camp, services provided, cctv etc. A panoply of technologies constituting a key spending of the 1,5 billion euros the EU spend annually on Research and Development for Security Technology.

Within the member States’ borders, people applying for asylum are submitted to speech recognitions technologies which have proven to be deficient to locate their regions of origins.

The use of software on mobile phone devices is also being used which is GPS enabled, and it also sends out instructions to the person being tracked in Germany there have been successful cases won where the practise of extracting data from mobile phones in this was has been found unlawful (DFF, 2021). Sharing of a status of a person as undocumented by other public services is also taking place in Germany, where it is being currently challenged. The use of digital technologies in a context of criminalisation of migrants originating from the Global South is part of the reason why the European Union has the deadliest border in the world. It creates violent conditions of mobility for people- especially those who are not provided with safe passages into the European territories.

CASE STUDY : KENTAURUS AND HYPERION IN GREECE

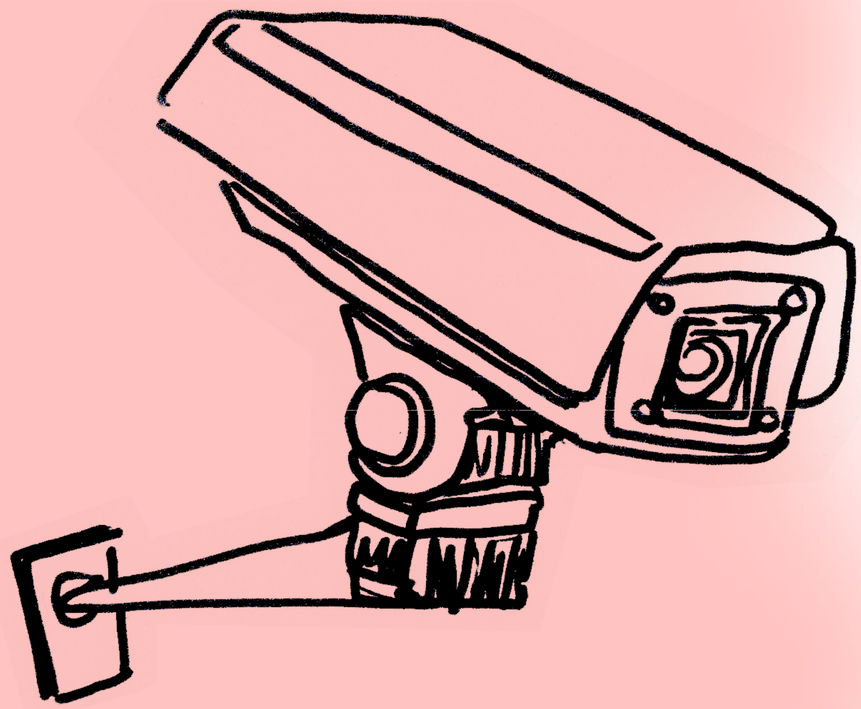
Hyperion was described by the hellenic of Digital governance for the area of migration and asylum as “an asylum seekers’ management system with regard to all the needs of the Reception and Identification Services. It (included) a detailed record of the data of asylum seekers and it (was) interconnected with the ALKYONI II system with regard to the asylum application. In addition, it (was meant to) be the main tool for the operation of all related facilities as it will be responsible for access control (entry – exit through security turnstiles, with the presentation of an individual card of a migrant, NGO member, worker andsimultaneous use of fingerprints), the monitoring of benefits per asylum seeker using an individual card (food, clothing supplies, etc.) and movementsbetween the different facilities. At the same time, the project include(d) the creation of a mobile phone application that will provide personalized information to the user, will be his/her electronic mailbox regarding his/her asylum application process and will enable the Service to provide personalized information.”

Centaurus was planned as “a digital system for managing electronic and physical security around and inside the facilities, using cameras and Artificial Intelligence Behavioral Analytics algorithms. It include(d) centralised management from the headquarters of the Ministry of Digital Governance and the following services: Signaling perimeter breach alarms using cameras and motion analysis algorithms; signaling of illegal behavior alarms of individuals or groups of individuals in assembly areas inside the facility; and use of unmanned aircraft systems to assess incidents inside the facility without human intervention, among other functions”

■ The Hellenic DPA is requested to take action again the deployment of ICT systems IPERION & KENTAUROS in facilities hosting asylum seekers in Greece, Homo Digitalis Website consulted in June 2024.

“People on the move, such as asylum seekers, are targeted by these intrusive technologies. Strong evidence has shown that the deployment and use of such surveillance technology could increase state surveillance on marginalised communities and lead to human rights infringements. It is important to highlight that KENTAUROS and HYPERION are not the only technology-led border management tools deployed in border management procedures in Greece. In 2021, the Hellenic Police acquired smart policing gadgets, which allow for the use of facial recognition and fingerprint identification technologies during police stops targeting undocumented migrants living in the country. Moreover, the Hellenic Coast Guard has contracted a private vendor to develop an AI social media monitoring tool.

■ “Greek Ministry of Asylum and Migration face a record-breaking €175,000 fine for the border management systems KENTAUROS & HYPERION, EDRi website, consulted in June 2024.



DIGITAL POLICING of PLACE

In this section, we *think* about *how localities* are digitally policed through *video surveillance*, *predictive policing technologies* and online policing.

Locality policing

has always been something that has been focused on for street level policing, but the digital policing is happening in full force through various methods of technology. Video surveillance, predictive policing, databases, handheld devices, algorithmic surveillance, biometrics. All of these tools are being used to digitally police communities on a local level.

Locality policing is the deployment of policing resources to a specific geographical area and usually involves surveillance and enforcement that leads to targeted strategy, and operations as well as the creation of "hot spot" areas' and facilitates over policing and criminalisation.

Technology plays a large part in locality policing as alongside police officers on the ground, there is the use of video surveillance, predictive policing, databases, devices, and algorithmic surveillance biometrics. Algorithm indicators such as areas with high populations of racialized communities, previous criminal activity, areas with high levels of unemployment and poverty will flag areas, placing those who live or move through these areas as high risk, undesirables, who need higher and more intense levels of policing.

A common example of locality policing, or hotspot areas concerns social housing estates, where there will be a consistent presence of digital policing and street level policing. This presence of digital policing tools will lead to increased levels of stop and searches, vehicle stops, harassment, use of GPS ankle monitors, specific crime based operation. It will also lead to increased policing and enforcement from other state agencies such as social services, and immigration enforcement.

"In Rotterdam, a large city which has large communities of migrants and first and second generation Dutch people who are racially minoritised, the police is using predictive policing systems and detection softwares which they have implemented to focus on anticipating incidents or people involved in serious violence. For example there is one algorithm which is used to detect who is carrying a firearm, and this is done through place based geographical location and their ethnicity: Moroccan, Somali, or Antillians. This just demonstrates how the intersection of the criminalisation of poor racialised communities works, by using those two characteristics are a determination of risk"

Nawal Mustafa,
PILP
2023

“In Denmark, there are geographical areas that have led to be known as ‘ghetto zones’ or ‘harsh penalty zones’. These areas have specific social criteria such as a population with over 50% non-Western immigrants, more than 2.7% of people have criminal convictions, or inhabitants have less than 55% of the gross average income in the region. There is also the belief that the immigrants living in these concentrated areas do not wish to integrate into Danish communities. It can be believed that racism underpins their precarity and xenophobia the subsequent policing and criminalisation of these communities where there is widespread introductions of monitoring and surveillance taking place”

Patrick Williams,
2023

PREDICTIVE POLICING

Predicting policing is the term used to describe policing institutions activity

which attempts to predict future criminal activity by using algorithms and previously recorded data.

The police use pre existing crime data, often provided by private companies, and international agencies to predict and identify where and/or when crime will take place, or predict who will commit crime. These predictions are based on harmful narratives which are often highly racist, classist and result in specific and targeted policing of areas where there are high levels of poverty, diasporic communities which leads to further marginalisation of people who are present or living in these areas (DFF, 2020).

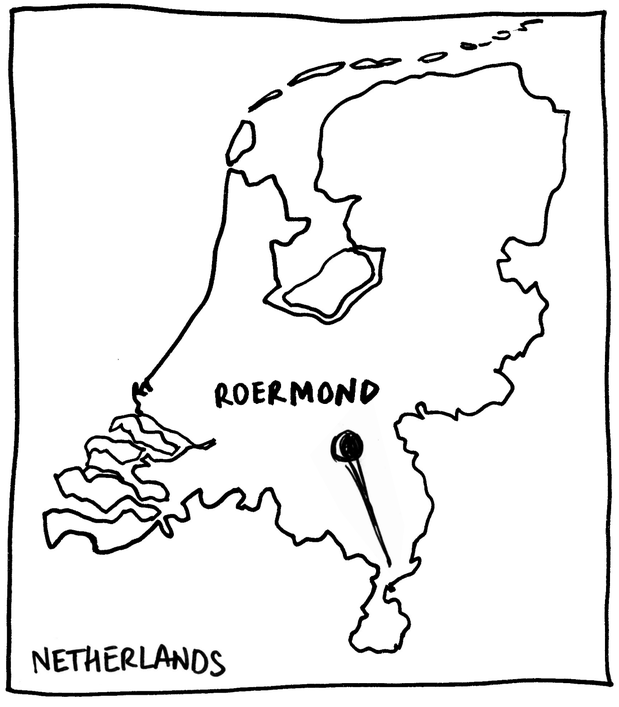
In France there is the increasing digital surveillance of public urban space, with tech imported from Israeli companies being used across the country and creating what has been referred to as "Smart Cities", hundreds of millions of euros are invested into the development and implementation of softwares which are being used to enable predictive policing in combination with algorithmic surveillance online to track individuals and groups. ■ (Felix Tréguer, La Quadrature du Net, 2018)

Predictive policing systems are being used to anticipate crime, in areas that are already overpoliced, and have been found to be most likely implemented in areas where there are large communities of racialised people living and can increase arrests by up to 30% (ENAR, 2019). It enables the the criminalisation of poverty and marginalised communities, and is used across migration enforcement. ■ (Lau, 2020)

"Technopolice was created because of the realisation that digital surveillance of urban spaces was being used to enable predictive policing platforms, and we felt like not enough was being done to fight against it, but we felt like we didn't know enough so started deeper exploratory work by using Freedom of Information Requests (FOI's) to get information. The FOI's was the first step, from this we moved to a public meeting, and connecting with others who were doing complementary work, which then led to connections with local grassroots groups and collective action being taken"

Felix Tréguer,
Technopolice

CASE STUDY: SENSING IN THE NETHERLANDS



In Roermond, Netherlands, at the border of Germany and Belgium, there is a shopping centre which attracts around 8 million visitors each year. The local police registers between 310 and 440 suspects of shoplifting or pickpocketing, per year. According to the statistics of the police detailing the nationality of the suspects, around 60% of them are of Dutch nationality. "However, the internal study conducted by the police, as well as the Sensing project in general, focused on 'mobile banditry', a concept generally used by the police for various economic crimes committed by foreign groups of so-called'bandits'. The police claim that most of the time, 'mobile banditry' is committed by persons coming to the Netherlands from Eastern European countries. (...) The police argue that shoplifting by 'mobile bandits' in Roermond specifically is committed mostly by people with Romanian nationality. For the Sensing project, the police have translated a target profile of pickpockets and shoplifters that fulfil the criteria of 'mobile banditry' into a set of criteria in an algorithm. These criteria consist of simple profile rules that can be matched with information from police databases and the aforementioned sensors that collect data in and around the city of Roermond (...) The predictive policing system makes use of police records and data collected through new and existing sensors installed in public spaces. These sensors include Automated Number Plate Recognition (ANPR) cameras, as well as cameras that are able to detect a vehicle's brand, model, year of manufacture, and colour. The collected data is then analysed using big data analytics and algorithms."

People who travel in groups and by car, have a German or Romanian license plate, travel through a specific route, use a car rented in Germany, might be in a stolen vehicle will be flagged high risk. Then a police officer has the opportunity to accept the call or not. "In practice, when the officers do respond, they will perform a final visual check to see if they think it is worthwhile to stop a car with these specific passengers in the context of the prevention of 'mobile banditry'. This depends on whether the passengers meet their subjective predetermined conceptions of what a 'mobile bandit' looks like".

■ All the quotes are from the Amnesty International report "We sense trouble: Automated discrimination and mass surveillance in predictive policing in the Netherlands", 2020.

CASE-STUDY: THE 400 IN THE NETHERLANDS

"The Top400 is a list of "high potential" children and youth who have not been convicted of high-impact crimes (unlike the Top600). The children and adolescents are monitored by, among others, the City of Amsterdam, the police, GGD and youth protection. A director is assigned to them who, among other things, discusses their progress within a core team of chain partners. According to the municipality, the goal of the Top400 approach is to prevent these young people from coming into contact with the police around high-impact crimes. For placement on the Top400 list, criteria have been developed that the children and youths must meet. The so-called "ProKid+" algorithm was also used to supplement the list and place 125 children and youth on the list. The Top400 approach also "includes" younger siblings, even if they do not meet the criteria." ■ Pilp.

"There is an absence of data on the ethnicity and socio-economic status of those on the Top400. The documents merely mention that. ethnicity and nationality are not included in ProKid+. However, the geographic distribution of the Top400 reveals that the distribution of minors is skewed towards the low-income and migrant neighbourhoods of Amsterdam (...) Once selected, a minor and young adult will be part of the Top400 approach for a minimum of two years. The behaviour of the persons, as registered in police databases, will determine whether this period gets extended. The directors made the following observations (...) Who are these at-risk minors and young adults? According to the documents, the minors and young adults selected for the Top400 can often be found on the street, where they display criminal behaviour and show worrying signs, such as public displays of anti-social behaviour, debts, school absenteeism and, oftentimes, slight cognitive disorders"

■ Top400, a Top-down crime-prevention strategy in Amsterdam, Fieke Jansen.

ALGORITHMIC VIDEO SURVEILLANCE

Algorithmic Video Surveillance is the act of recording, storing and processing footage (data), on a larger scalea scale for which human surveillance only wouldn't be possible.

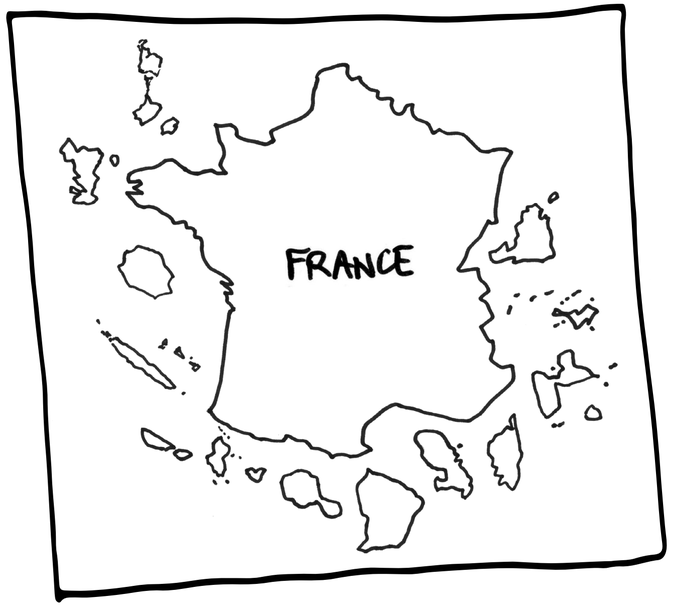
La Quadrature du Net defines algorithmic video surveillance as follow "the automation of the analysis of CCTV images thanks to a software that produce notifications when it detects an event that it has been trained to recognize.This analysis work was previously done by humans (municipal agents within urban supervision center or security agents within supermarket or private establishments). These softwares are based on so called 'computer vision' algorithms, a technology built on statistical learning that makes it possible to isolate meaningful information from static or moving images. In order to isolate these informations, algorithms are trained to automatically detect, through video streams from CCTV cameras, certain categories of objects (trash, bag), people (lying on the ground, graffiti artist, static person) or events (crossing a line) for instance." Persistent investment in counter terrorism laws across Europe and surveillance technologies is increasing the risk posed to racialised communities who are targeted under policies implemented to fight terrorism.

"While video surveillance is obviously everywhere we are seeing specifically targeted placement in communities that have high Black and brown populations, like in Rotterdam. We have to increasingly be aware how this kind of public policing is also folding into the digital policing in other spaces"

Nawal Mustafa, **PILP**

Globalisation is a key driving force in roll outs of Big Tech across Europe, software like that from US owned company Palantir, which is on the verge of being rolled out across Germany. This software has been said to use surveillance cameras and public records to coordinate data, but activists, and community members have worked with German Society for Civil Rights to highlight and argue that the software can also use social media and vehicle navigations systems (Knight, 2022).

CASE-STUDY: FRANCE LEGALISATION OF ALGORITHMIC VIDEO SURVEILLANCE



"The bill (concerning the Olympic game) approved the use of algorithmic video surveillance, a predictive surveillance technology that attempts to detect "pre-determined events." (as an experimentation). It does so by monitoring crowds in real time for "abnormal behaviour and crowd surges" and analyzing video data from drones and CCTV cameras. French technology lawyer Arnaud Touati explained that the "algorithms used in the software are notably based on machine learning technology, which allows AI video surveillance, over time, to continue to improve and adapt to new situations." Although Article 7 prohibits biometric data processing, facial recognition technology, and "interconnection or automated linking with other processing of personal data," it "necessarily [requires] isolating and therefore identifying individuals" through gait and other physical characteristics. The law will remain in effect through March 2025, several months after the Olympics finish. While Article 7 (of the bill) is new, France has a long history of police surveillance that dates back centuries. In the late nineteenth to early-mid twentieth centuries, police kept detailed records called the National Security's Central File, which was comprised of files on over 600,000 "anarchists and communists, foreigners, criminals, and people who requested identification documents." In the 1970s, after public outcry against the French government's attempts to centralize files on all citizens through its SAFARI program, France walked back its mass surveillance efforts."

■ Playing Games with Rights: A Case Against AI Surveillance at the 2024 Paris Olympics, Nteboheng Maya Mokuena, Georgetown Law technology Review website, consulted in June 2024.

Although there are no State collected statistics on race in France, the experimentation has been deployed in Seine-Saint-Denis, the department in France with the highest proportion of people with sub-saharan African origins.

ONLINE POLICING

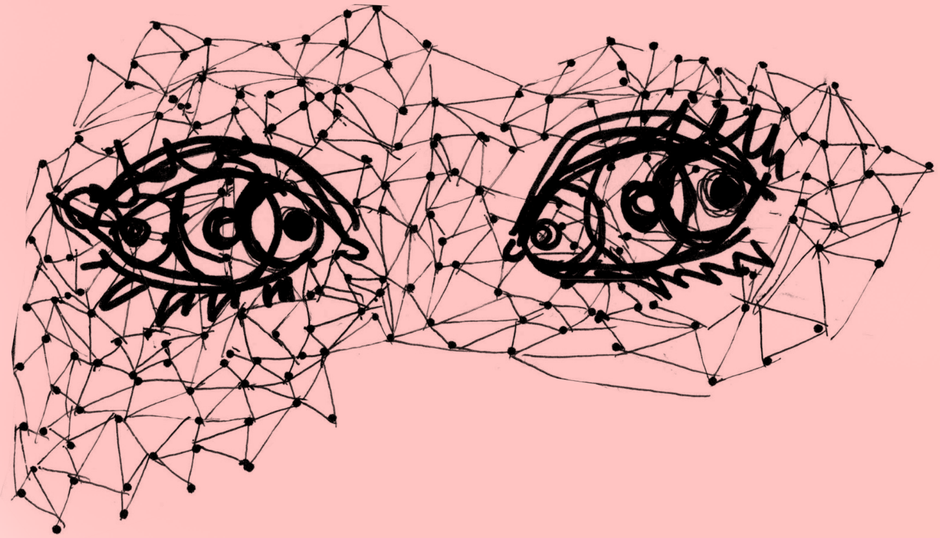
Our personal use of social media is now often policed not only by the police, but also by immigration enforcement and employers. We have seen this most recently with the recent uprisings and mobilisations for a Free Palestine, where individuals are expressing personal support online, and being punished in places of education (Rehman, 2023), fired from their places of work (Milman, 2023) or losing funding. In the UK, the Metropolitan Police are using social media accounts to find photos of organisers, and share their pictures for public support in investigations to enable prosecution which could trigger immigration enforcement also (ITV, 2023).

Online Activity That Causes Harm

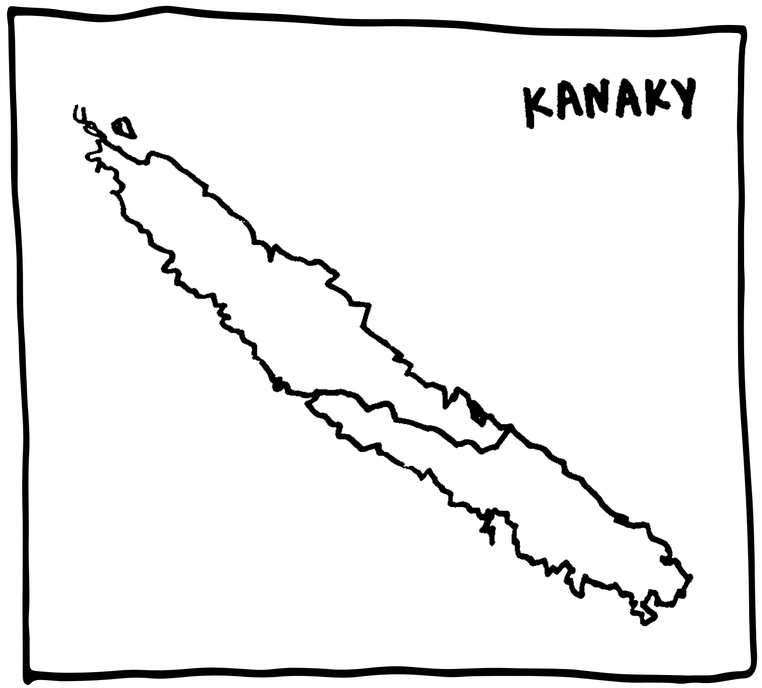
Hate speech is widely understood to be, offence discourse that targets a group or individual based on specific characteristics such as race, religious beliefs, or gender, which is used to cause harm, discriminate or incite hostility and violence (UN, 2023).

There is much focus on hate crime in mainstream, but without one universal definition, little to no structures to prevent it, and government officials who increasingly incite violence we believe that it's important to take a wider lens around online activity which causes harm.

With white supremacy at the root of narratives which cause oppression and harm, there has been consistent growth and tolerance for this across social media and results in the dehumanisation of racialized people, and in combination with other marginalised characteristics, and influences people to cause harm on a daily basis, both online and offline (Glitch, 2023).



CASE-STUDY: SHUTDOWN OF TIKTOK IN KANAKY/FRANCE



"On May 13, widespread protests erupted in New Caledonia over a new set of controversial voting reforms French authorities introduced to allow more people of European and Polynesian descent to vote in elections. New Caledonia is recognized as a non-self-governing territory by the UN Special Committee on Decolonization, but has been in a formal process of transition and decolonization with France since the signing of the Nouméa Accord in 1998. The process of independence has been subject to referendums which took place in 2018, 2020, and 2021, the last of which was forced by France at the height of the COVID-19 pandemic. As a result, there was a boycott by pro-independence groups, and the legitimacy of the vote is highly contested. Independence activists fear that recent reforms will dilute the political representation of the indigenous Kanak people, who make up 41% of New Caledonia's population.

The TikTok block was implemented by the state-run Post and Telecommunication Service, the single internet service provider for New Caledonia, impacting mobile services managed by operator Mobilis across the entire territory. Direct testimonies from people in the area stated that the app was accessible, but that feeds were empty and there was no content available. Neither French Prime Minister Gabriel Attal nor New Caledonian High Commissioner Louis Le Franc gave an explanation for why TikTok was chosen. According to the former president of New Caledonia, Phillipe Gomes, the TikTok block was aimed at stopping protesters from "organizing reunions and protests." With seven people killed and hundreds injured since May 13, it's clear that blocking TikTok did not stop protests, nor did it ease tensions or prevent violence. After visiting New Caledonia on May 21, French President Emmanuel Macron ultimately delayed the voting reforms but insisted that they would eventually move forward."

■ First-time culprit: France blocks TikTok in New Caledonia, Access Now, 5 June 2024.