

**WEAVING
LIBERATION**

RESISTING DIGITAL POLICING IN EUROPE

A Toolkit

CREDITS

This toolkit was thought, written and designed by Zara Manoehoetoe with the support of Laurence Meyer. It was reviewed by Laurence Meyer who also added the case studies. Adelaide Hirwe (Weaving Liberation) did the coordination work between the different actors and supported the research work.

Visual identity is by Alice Z Jones. Art direction, illustrations and graphic design by Claire Zaniolo & Estelle Ndjop Pom.

FOREWORD

Laurence Meyer,
Co-director
Weaving Liberation



The genesis of this toolkit is an on-line Digital Policing workshop, as part of an early series of workshops from the “Digital Rights for All” initiative. The participants expressed the need to have a document which gave an overview of the different digital tools used to reinforce policing as a mean to surveil, control and coerce. Two years later, with many more “Digital Rights for All” workshops behind us and a more recent gathering on Digital Policing, this time in person under Weaving Liberation’s hat, this toolkit is finally seeing the light of day. It brings together the work of many others on the subject, a series of interviews led by Zara Manoehoetoe, and case studies. The second part proposes tools of resistance, because we can resist. These tools of resistance are also inspired by previous practices and the work of others.

Digital policing is a part of traditional policing, it participates in producing the framework of crimes and thus of the “criminal”. Crimes and harms are never synonyms. For a long time in Germany, until 1992 in fact, the law considered that a woman couldn’t be raped by her husband. In many countries, crossing borders constitutes a criminal offence although no harm has been done. Decoupling harm from criminal frameworks is important to question the appropriateness of the response. In many countries sex work is criminalised, though it has been shown that this

3
criminalisation harms sex workers. It invites us to ask the question: is criminal law the best vehicle to repair and prevent harm? Feminist studies have largely showed how criminal law often puts the victim on trial, creating more harm. Critical legal studies in general and critical race theory in particular, have been instrumental in demonstrating that criminal law not only fails to apply equally to all, it also functions as an instrument to reinforce inequality. In the part of the toolkit on “What even is Digital Policing?”, information is shared on what an abolitionist perspective of policing is and why that is the perspective adopted in this toolkit. For now, mentioning this fundamental difference between criminal law, which enables law enforcement authorities to have “the monopoly of legal violence” as Weber states, and harm, allows us to interrogate how, rather than repairing or preventing harm, law enforcement equipped with digital tools can instead enables human rights violations. It is important to add that in an ideal society, policing is indeed obsolete – the goal we all are striving for is resolutions of conflicts that do not need the use of legal violence – we would all prefer to have less weapons rather than to have militarised forces with the mission of protecting us.

Digital policing can create and perpetuate discrimination, both through discriminatory enforcement and as a tool

of criminalisation – those two mechanisms are not exclusive from one another but rather complementary.

1. Digital policing as a tool of discriminatory enforcement

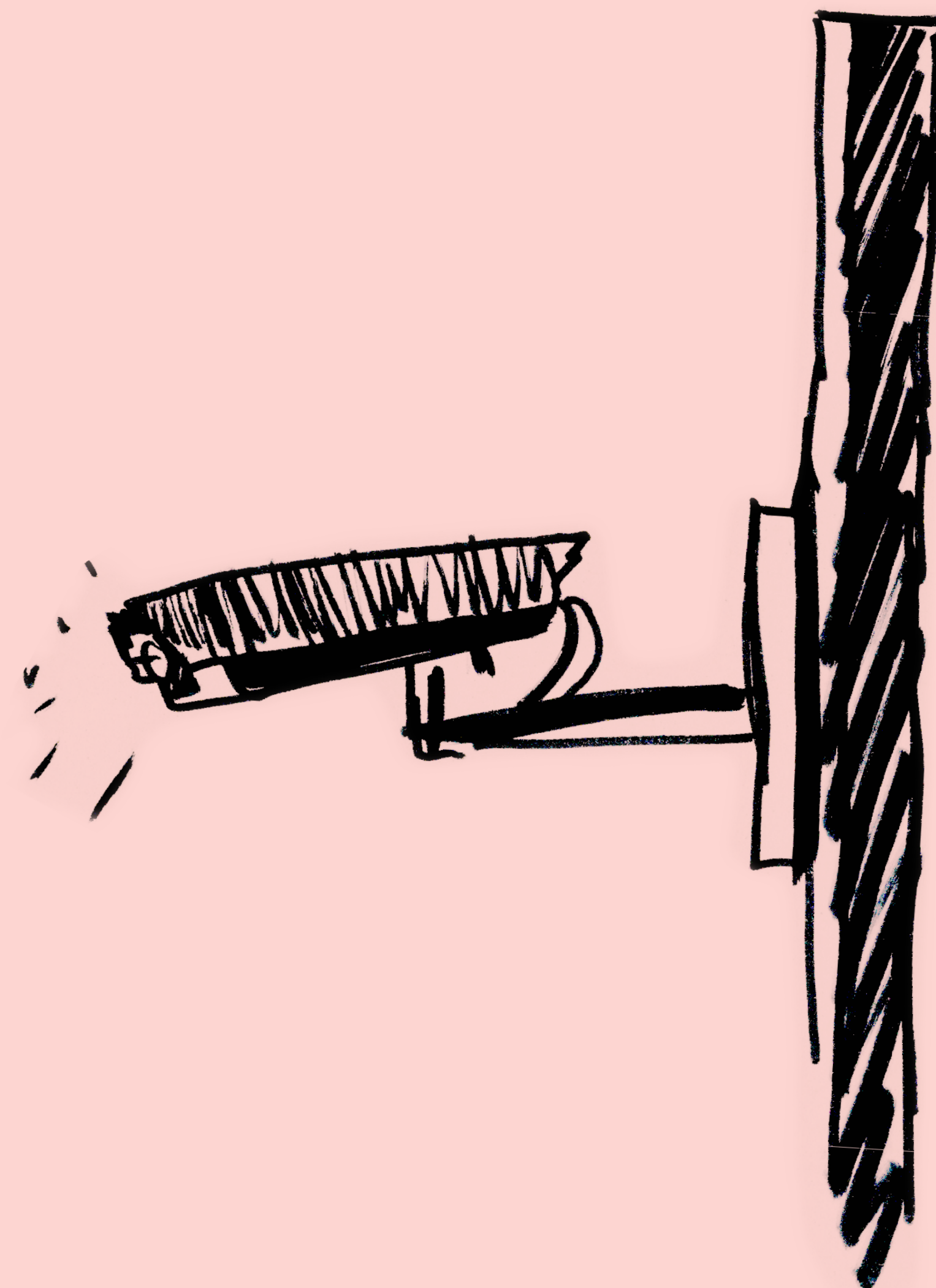
As you will see throughout this toolkit, different tools used in digital policing are presented. Many of them enable a discriminatory enforcement of the law. In cases of predictive policing or when concerning welfare, for example (p. 26 and following), the technological systems only work using frameworks which were already in place and part of the mechanics of law enforcement or social service. In the case of *Sensing* for example, the algorithm is set using criteria developed for “mobile banditry” already imbued with xenophobic prejudices.

Moreover, when an algorithm is used to calculate risk (e.g., risk of fraud, risk of committing a crime, etc.), the decision to act upon the flagging relies on individuals. It is a person who has to decide whether to take into account what has been flagged. This is one of the elements that was put in place in the GDPR as well as other subsequent legislations around automated decision-making systems as safeguard. Though it has advantages, one of which is allowing the ability to trace legal responsibility back

to a physical person and/or an institution, it fails to take into account how those services worked using discriminatory frameworks before they used algorithmic supports. In *Sensing*, in the Gang Matrix, in the algorithmic system used concerning social benefits in Rotterdam... the use of technological tools enable automatisations and therefore amplify existing discriminatory practices, though the law they aim to enforce doesn't directly discriminate. Hence for example, when the aim in the *Sensing* case is to prevent shoplifting, the specific ways the tools were used led to discriminatory enforcement.

2. Digital policing as a tool of criminalisation

In many of the cases you will read about, digital technologies are used to detect what is deemed as suspicious behaviours and prevent crimes from happening before they happen. The discourse around the preventive potential of digital technologies in policing centres on the idea that surveillance creates safety on one hand and, on the other hand, that some profiles are more prone to become criminals. What we see is that the use of those technologies, using the concept of prevention, are often enabling criminalisation, mainly of racialised and/or impoverished communities.



In the example of the Gang Matrix, young people, and overwhelmingly Black men, were put in a database meant to identify gang members, many without having any prior criminal record. In the Top400 case in Amsterdam, young people who are deemed to show “deviant behaviours”, again in a highly racialised and impoverished neighbourhood, are put under specific scrutiny and added to a specific programme. In the child benefit scandal in the Netherlands, people, again often racialised, were wrongly accused of fraudulent activities. These technologies rather than preventing harm from happening, exacerbate the identification of certain communities with criminality, pushing people into the criminal box. This demonstrates once again that crime is not a neutral concept but rather one that is used to control, surveil and sanction, not necessarily in connection to harms being done. These mechanisms are not specific to the technologies but mirror historical logics in policing which informed the construction of racial hierarchy (Muhammad, K. G. 2010; Browne S. 2015).

As a tool of criminalisation, it heightens surveillance of specific groups without increasing safety. Rather, to the contrary: a high rate of criminal offences recorded will justify the deployment of digital tools used in policing, which will in turn create a zoom-in effect on criminalisation in that area, which will

then justify an increase in policing, etc. Hence, criminalisation, not safety, is a key driver for the increase of digital tools of surveillance and risk-assessment.

3. The structural issue of access to justice with regard to human rights violations in digital policing

In a lot of the cases shared in this toolkit, a common thread is the feeling of opacity. It could be that people are unknowingly being handled with the support of digital technologies (e.g., Gang Matrix, risk-assessment algorithms in the Netherlands etc.). It could be that though they are aware of the use of digital technologies, the functioning of those tools and the ways they will impact them remain opaque. The use of digital technologies in the context of policing leading to discriminatory impacts is all the more worrying, given that not only a technical but a legally organised opacity makes it hard to challenge it.

In the GDPR, exemptions are made to the protection awarded in the text in some of its articles in matters of, “safeguard (of) national security; defence; public security; the prevention, investigation, detection or prosecution of criminal offences or the execution of



criminal penalties, including the safeguarding against and the prevention of threats to public security” as stated in Article 23.

When an individual tries to know if and what type of information about them is being stored by EUROPOL, Article 36 of the EUROPOL Regulation enables the agency to decline a request in order to “enable Europol to fulfil its tasks properly; protect security and public order or prevent crime; guarantee that any national investigation will not be jeopardised; or protect the rights and freedoms of third parties.” This leaves a substantial margin of appreciation. In the same vein, the AI act foresees in its article 14 (5) specific exemptions, even concerning systems classified as high risks used for the «purposes of law enforcement, migration, border control or asylum where Union or national law considers the application of this requirement to be disproportionate». Those high risks systems, which many pleaded to prohibit due to their high probability of serious human rights violation (see Sarah Chander and Alyna Smith «As AI act votes near, the EU needs to draw a red line on racist surveillance») are

for example so-called «lie detectors» or «language recognition systems». All of which have proven to have harmed asylum seekers in their quest for protection. This opacity is largely organised legally but is also the result of illegal actions by law enforcement. In the first decision of the European Court of Human Rights regarding facial recognition technology “GLUKHIN v. RUSSIA” the use of facial recognition technology to identify and pursue a political opponent was deduced from the situation. In 2021, the European Data Protection Supervisor found major compliance issues with the EUROPOL regulation in the way EUROPOL collected data, often out of the scope that was authorised. In Sweden, law enforcement forces were fined for using the Clearview AI algorithm illegally. This opacity creates barriers to access justice for multiple reasons. Firstly, it makes the gathering of evidence highly complicated, especially in cases of discrimination for which the discriminatory impact must be shown and therefore necessitates data to compare and prove the unequal treatment. This is linked to another barrier: the individualisation.

Although the harms caused by digital policing impact communities (improved, racialised communities –among them single mothers, migrant communities, young racialised men, etc.) and target spaces which, by definition, are collective (neighbourhoods, malls, etc.), the legal means designed to denounce these harms rely on individual action in front of jurisdictions. These legal pathways are often cumbersome and hard to decipher for many, especially for marginalised communities who have fewer legal experts in their circles. They are costly in time and money. Finally, it produces fear. Marginalised communities are facing what is presented to them as an implacable and complex machine, producing results that they have to accept although they know them to be wrong – profoundly Kafkaesque situations for people whose lives are marked by constant precarity.

These barriers work as disincentives, discouraging people to claim their due rights. When they do, the legal systems still often fail to offer adequate remedies that not only would repair the harm done but also prevent it from happening again. We see it with the hydra

that have proven to be the algorithms used to assess risks of frauds in welfare systems. Despite the Syri decision in the Netherlands, those systems have continued to flourish, not only in the Netherlands, but also abroad, with cases in France now, for example.

This paints a grim picture. But in reality, people are nonetheless resisting. That is how, in most cases, we know of abuses – because people notice something and they talk to one another, because they meet and do not accept the injustices they face, because they talk in community and in movements, build knowledge and debunk myths. These oppressive technologies can only be challenged when the impacted communities tell what is happening – flagging the flaggers; when they organise, when they see a chance to win. Without community there is no justice. The second part of this toolkit is all about this.

Laurence Meyer

METHODOLOGY

Zara Manoehoetoe,
part of Northern Police
Monitoring and Kids of Colour

Community organisers, activists, and affected community members have made clear, especially over the last few years, the growing need to increase understanding of what digital policing means, the mechanisms of it, technologies used, and the impacts it has, so that we are collectively better positioned to resist it.

Our first objective for the toolkit was to grasp the level of knowledge that people affected by and those working to resist digital policing have. This was done by DFF through a series of conversations, events, and research, involving community members, activists, and academics from around Europe. One thing that really stood out was that people were really only fully understanding after harm had taken place, and were then finding themselves in a position having to respond.

The development of the digital policing tech happens at such a speed that it grows on a daily basis. When asked, people have told us how overwhelming,

intimidating and isolating it feels. And we are not surprised because the tech is intimidating. It became apparent that the last thing those affected by the digital tech the most, and those organising around it needed was some kind of leaflet or booklet which regurgitated academic journals and tech jargon manuals, but something that offered information, examples, practical tools, and ideas on how to build and resist- and so the idea for a toolkit was born.

The content of this toolkit has been developed through a variety of methods. Publications, articles, academic research has provided some of the content, but the richness, and the deeper and realistic understanding of how digital policing tech harms, and how we can work, together, to resist it has come from interviews with people who are working on the ground in support of those harmed by policing across Europe and in the US. By holding conversations and interviews with activists, community organisers, researchers, academics, people employed by NGO's, and

working within the legal field, we have been able to create this toolkit.

A toolkit which offers an overview of what digital policing is and aims to do, different types of technologies used by policing and enforcement agencies, how they are used to harm people, how we can resist, and the importance of building a collective and international movement, and cross movement solidarity.

It wouldn't have been possible without the engagement of Eleftherios Chelioudakis, Alyna Smith, Nawal Mustafa, Laura Rivera and Sejal Zota, Griff Ferris, Felix Tréguer, Esra Ozkan and Sanne Stevens, Patrick Williams, Catherine Barnett, Paul Day, Oyidiya Oji, and Sabrina Sanchez.

We thank every single person involved for their vital and insightful contributions and time!

Zara Manoehoetoe

“Awareness is key to building knowledge and power, so that we can equip ourselves within the tools we need to reduce the harm they are causing and work collectively on ultimately abolishing these practices”



**WHAT EVEN
IS
DIGITAL POLICING
TECHNOLOGY?**

BEFORE WE GET INTO IT, *lets give you some context* ↳ THE TOOLKIT...

This toolkit has been developed with an abolitionist understanding of policing, which considers the systems and mechanisms of policing to be inherently harmful (McDowell & Fernandez, 2018). From an abolitionist perspective, though policing is presented as a system meant to protect the public and prevent crime, the system of policing has historically and continues to work to uphold the law, protect the state and protect private property in a way that fails to create real safety (Day & McBean, 2022). Moreover, policing rather than achieving safety for all- tends to create harm especially in racialised, impoverished, disabled, queer, migrant communities and among people minoritised in their gender. Abolitionist approaches to policing also often stretch that policing didn't always exist and that in an ideal world police and prison shouldn't exist.

Du Bois (1935) explains that policing as we know it today is a legacy of colonial slave patrols, which were redesigned and developed to extend power to people employed by the state to control, repress, criminalise, and punish people. Still to this day, policing creates criminality in a way which targets, surveils and controls communities, without fundamentally addressing or repairing harm when harm is done. In short, from an abolitionist point of view, police doesn't prevent harm from happening, in many ins-

stances causes harm within specific communities and could be replaced by systems better shaped to create collective infrastructures of safety not centring State sanctioned violence. Abolitionist approaches are multiple and contextual and not always agreeing with one another. To learn more about them [Abolitionist Futures](#) has put together one reading list that can be consulted online here. While people may see the physical policing of our streets, lives, and borders, the tech that is used is often not highlighted or visible in the same way.

This toolkit aims to introduce different types of digital policing, highlighting the harms it causes, and steps we can take or tools we can use to fight back against its power, and build a stronger movement to resist it through and abolitionist social justice oriented lens.

DIGITAL POLICING...

“Policing in general, and digital policing specifically is a tool of oppression. A tool that is used to disproportionately harm people from the already most marginalised communities, in targeted ways for example the policing of Black communities, targeting migrants, or the criminalisation of poverty”

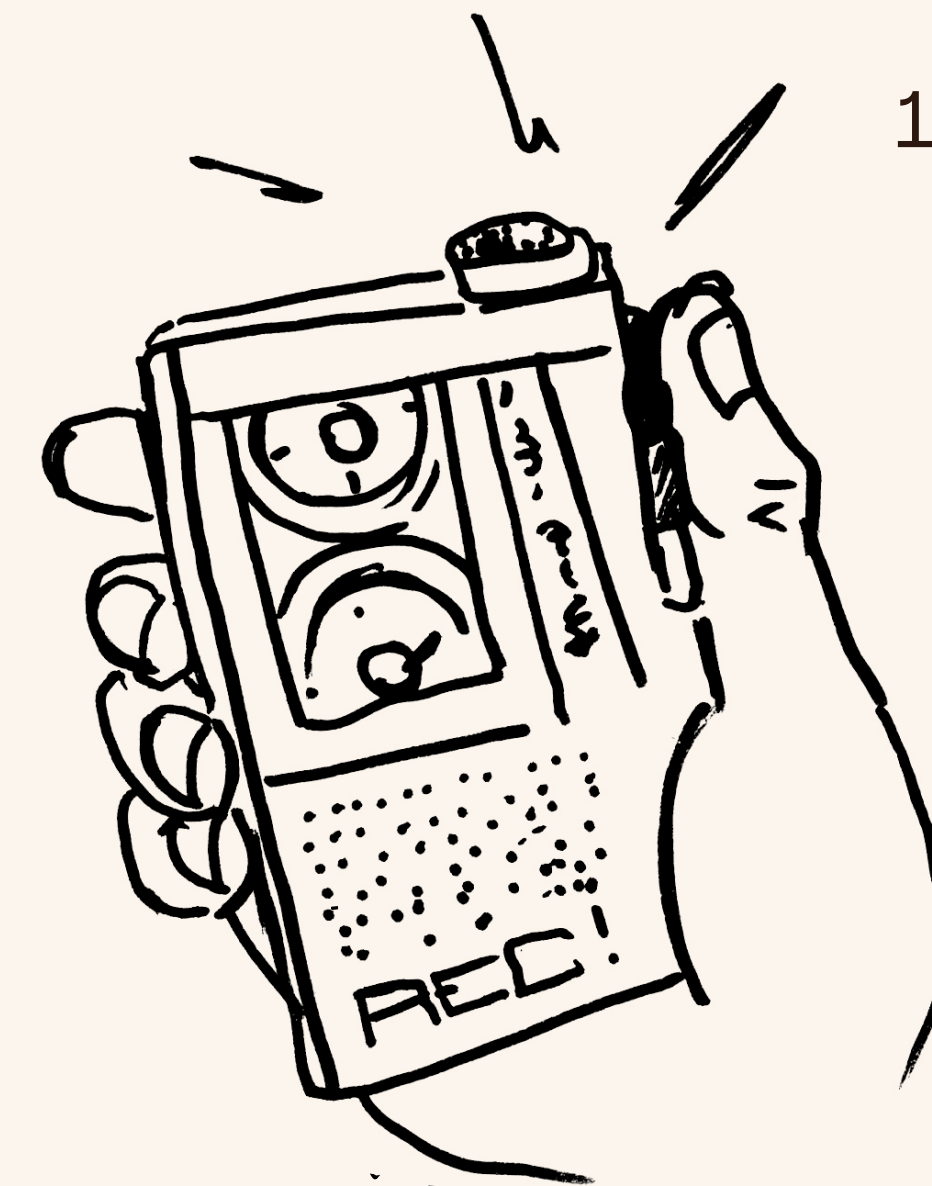
Digital Policing is a continuation and extension of the harmful system of policing. Simply put, digital policing is a term used to describe the wider modernisation of policing services (Kimbell, 2023), through technology (Weeks, 2022). The technology enhances the oppressive framework of a carceral State around which policing is built (Hamid, 2020). The use of digital technologies widens the reach and impact. Digital policing uses software designed to imitate human action but produces it at a larger scale and faster speed, including

real time tracking and monitoring programmed to make instant decision for on the ground policing action (Ozkan & Stevens, 2021).

Within this toolkit, the term (digital) policing extends beyond traditional boundaries, across the welfare state, into border (enforcement), education, health, housing, employment. It encompasses ways all the ways in which digital technologies are mobilised by public authorities to control, surveil and sanction.

WE ASKED ORGANISERS:

What are consistent questions communities have about digital policing?



Sejal Zota
and Laura Rivera,
Just Futures Law
2023

“How to recognise the tech, understand what it does, who is using it and what the impacts are. Especially as we live in such a technological age, and we are so heavily reliant on tech, people want to recognise the harm.”

Oyidiya Oji,
**European Network
Against Racism**
2023

“Many people don't know about the technology or how it works, so they need to know that and how they counteract digital policing and what tools they need to do it. They need to understand the power structures and how they can be removed.”

Paul Day,
Youth Worker
2023

“How we can protect young people from a power we don't understand, or technologies they are dependant on in life that can be used to criminalise them.”

EVERYONE is AFFECTED BY DIGITAL POLICING... *but* SOME, *more than* OTHERS...

12

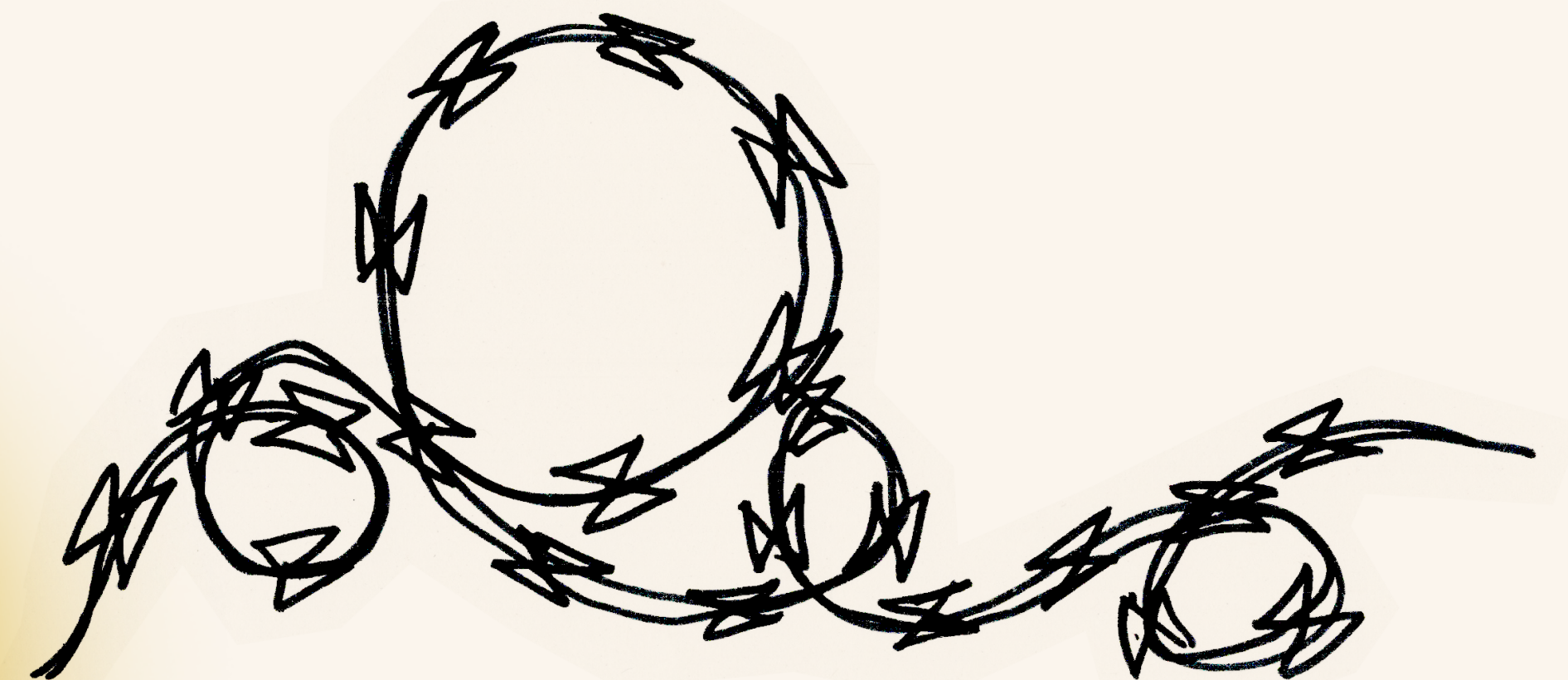
The assumption that humans need to be tracked to protect public peace and to prevent, deter or intervene in crime has led to invasive and excessive digital policing technologies and frameworks. The ability to track and monitor people in the modern age through cameras or access to personal data is a mechanism which enables and results in harm that does affect everyone, in some way.

We have been guided to become so dependant on technologies that a digital footprint is a natural outcome for us, but the hidden risks attached come at real costs. Whether it comes to travel, employment, housing, health, education, banking, **we often have to share our data to access services.** While it can sometimes seem to simplify things, it also makes us vulnerable to our data being owned, stored, manipulated, and sold and us being increasingly surveilled and controlled.

Because Collecting Data and synchronising databases create intelligence about our consumption habits, who we meet, how we meet them and how we move around— it has increasingly become a priority for the government, services, and across the private sector.

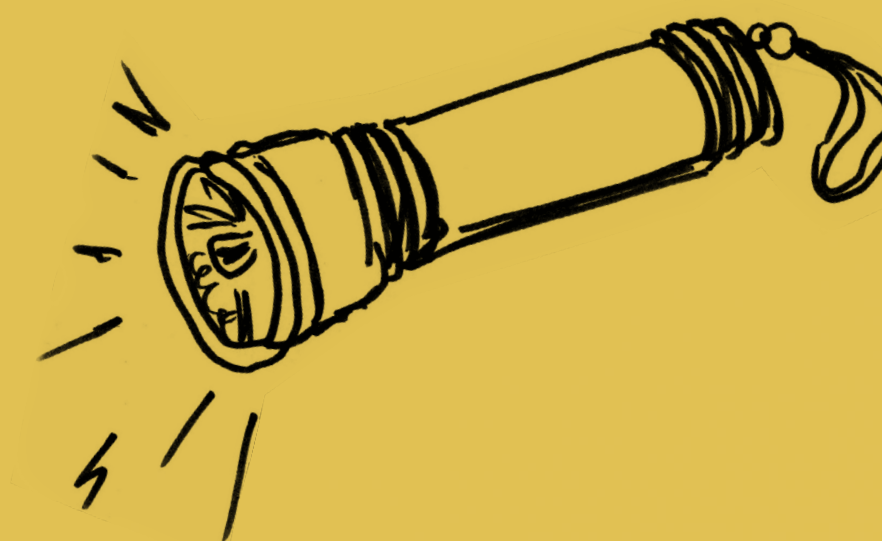
While we acknowledge that everyone is affected by digital policing we want to centre social justice values in this toolkit recognising that for some of us the effects are dangerous, and potentially life threatening.

We believe that to achieve liberation, we have to centre those most marginalised and at risk of harm. To resist digital policing effectively and collectively we must start from where the most danger exists.



TERMS AND DEFINITION

from the Racial Equity Glossary — Racial Equity tools



ABOLITION “The action of abolishing a system, practice, or institution. Abolition centers on getting rid of prison, jails, police, courts, and surveillance. Abolitionist practice is also about establishing a system that is rooted in dignity and care for all people. A system that does not rely on punishment as accountability.”

LIBERATION The creation of relationships, societies, communities, organizations, and collective spaces characterized by equity, fairness, and the implementation of systems for the allocation of goods, services, benefits, and rewards that support the full participation of each human and the promotion of their full humanness.

MARGINALISATION A social process by which individuals or groups are (intentionally or unintentionally) distanced

from access to power and resources and constructed as insignificant, peripheral, or less valuable/privileged to a community or “mainstream” society. This term describes a social process, so as not to imply a lack of agency. Marginalised groups or people are those excluded from mainstream social, economic, cultural, or political life. Examples of marginalised groups include, but are by no means limited to, groups excluded due to race, religion, political or cultural group, age, gender, or financial status. To what extent such populations are marginalised, however, is context specific and reliant on the cultural organization of the social site in question.

MOVEMENT BUILDING Movement building is the effort of social change agents to engage power holders and the broader

society in addressing a systemic problem or injustice while promoting an alternative vision or solution. Movement building requires a range of intersecting approaches through a set of distinct stages over a long-term period of time. Through movement building, organizers can:

- Propose solutions to the root causes of social problems.
- Enable people to exercise their collective power.
- Humanize groups that have been denied basic human rights and improve conditions for the groups affected.
- Create structural change by building something larger than a particular organization or campaign.
- Promote visions and values for society based on fairness, justice, and democracy.

WHITE SUPREMACY The idea (ideology) that white people and

the ideas, thoughts, beliefs, and actions of white people are superior to People of Color and their ideas, thoughts, beliefs, and actions. While most people associate white supremacy with extremist groups like the Ku Klux Klan and the neo-Nazis, white supremacy is ever present in our institutional and cultural assumptions that assign value, morality, goodness, and humanity to the white group while casting people and communities of color as worthless (worthless), immoral, bad, and inhuman and “undeserving.” Drawing from critical race theory, the term “white supremacy” also refers to a political or socio-economic system where white people enjoy structural advantage and rights that other racial and ethnic groups do not, both at a collective and an individual level.

LET'S BREAKDOWN WHAT TO EXPECT FROM THE TOOLKIT...



The toolkit has been designed and created to provide information and basic introduction to common digital policingtech, offer real life experiences of the impacts (harm) it causes, and demonstrate the way that (digital) policing is designed, implemented, and invested in to uphold white supremacist and exploitative interests. **The toolkit will highlight real cases in which public entities, be it national and international bodies, or private companies, produce marginalisation and harm, with the support of digital technologies.**

But this toolkit has been created with the belief, commitment and long-term vision of a safe world. Created with the abolitionist belief that, people, the public, you, us, will one day be liberated. The long-term goal is the dismantling of oppressive systems: reaching a place

where communities have worked together to build relationships, invest in healing, and create new infrastructures, mechanisms, services, and places of support, reaching a time where the weight of power has been tipped.

With this dream in mind, we take the learning from our experiences, from connecting with others, participating in resistance work, witnessing the wins that happen across organising efforts in Europe, and the globe, from living during these times of change, uncertainty, uprising, dissolution, widespread civil disobedience, intensified policing, and radical reaction.

This toolkit will offer, tools, ideas, examples, learnings, hints and reflections, to hopefully inspire or support others to engage in resistance.

SUMMARY

16

**How
Digital
Policing
Harms**

40

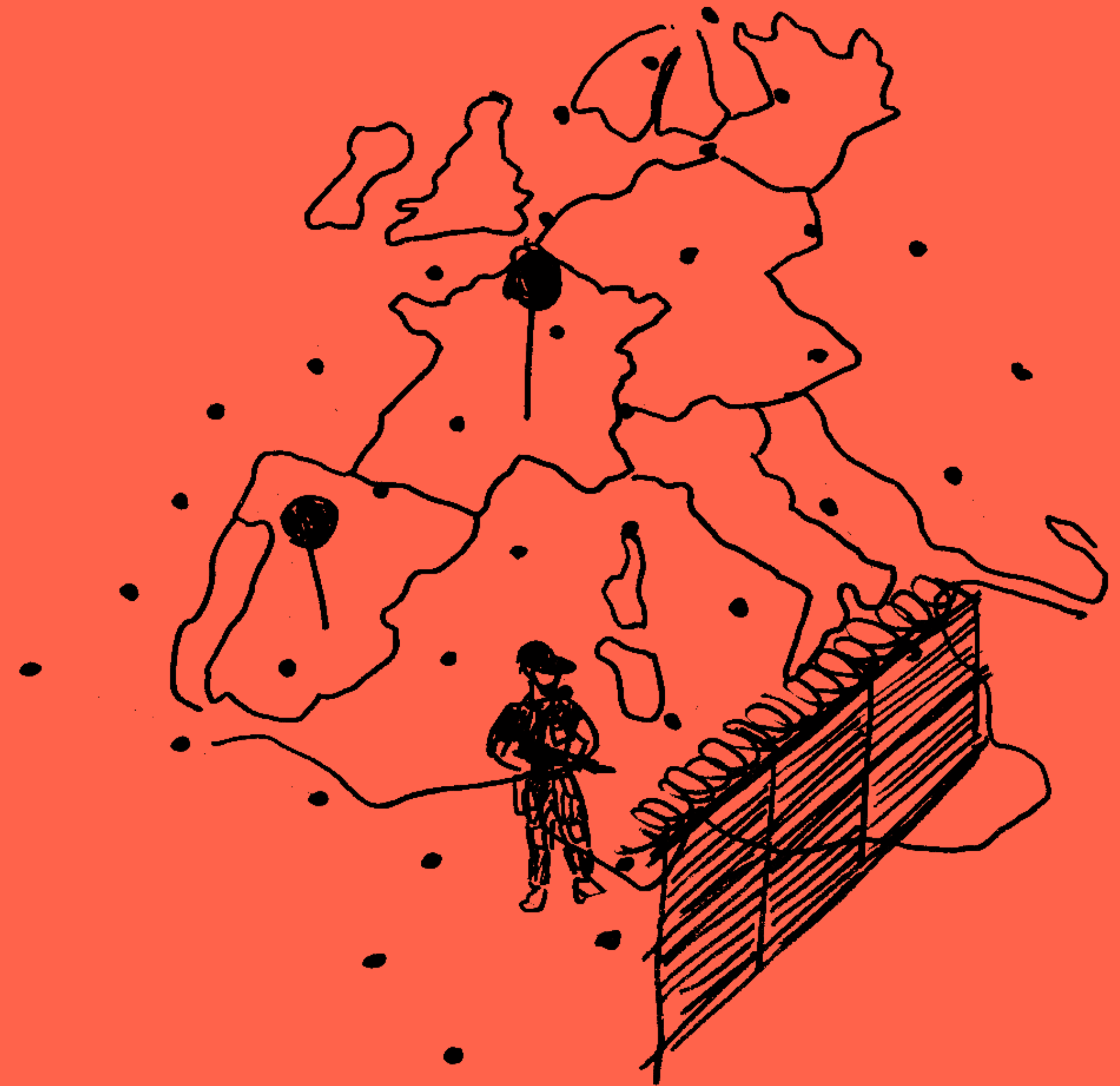
**Tools
Of Resistance**

65

**Building
A Movement**

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.”



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.

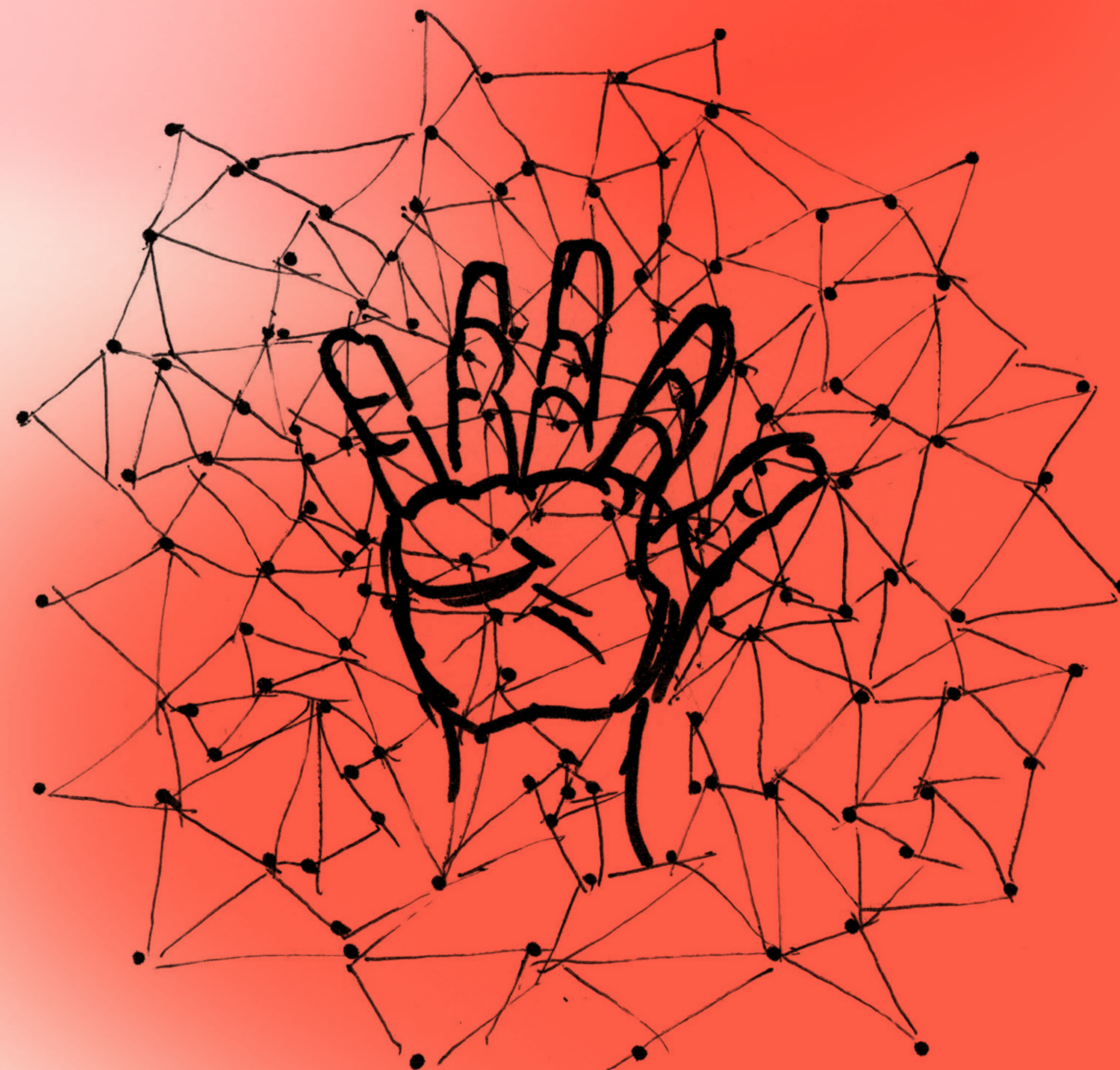
Fingerprints, DNA, or the eye (iris/retina) are types of biometric data and are used to verify people's identity. Development in technologies has meant that they are now able to also use behavioural data as biometrics, this includes voice recognition, signature dynamics, and even sounds of footsteps.

The practise of biometrics was used during transatlantic slavery, through the practice of branding the bodies of enslaved people (DFE, 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 themselves 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”

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.”

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 (Oracle, 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”

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 reimburse 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 investi-

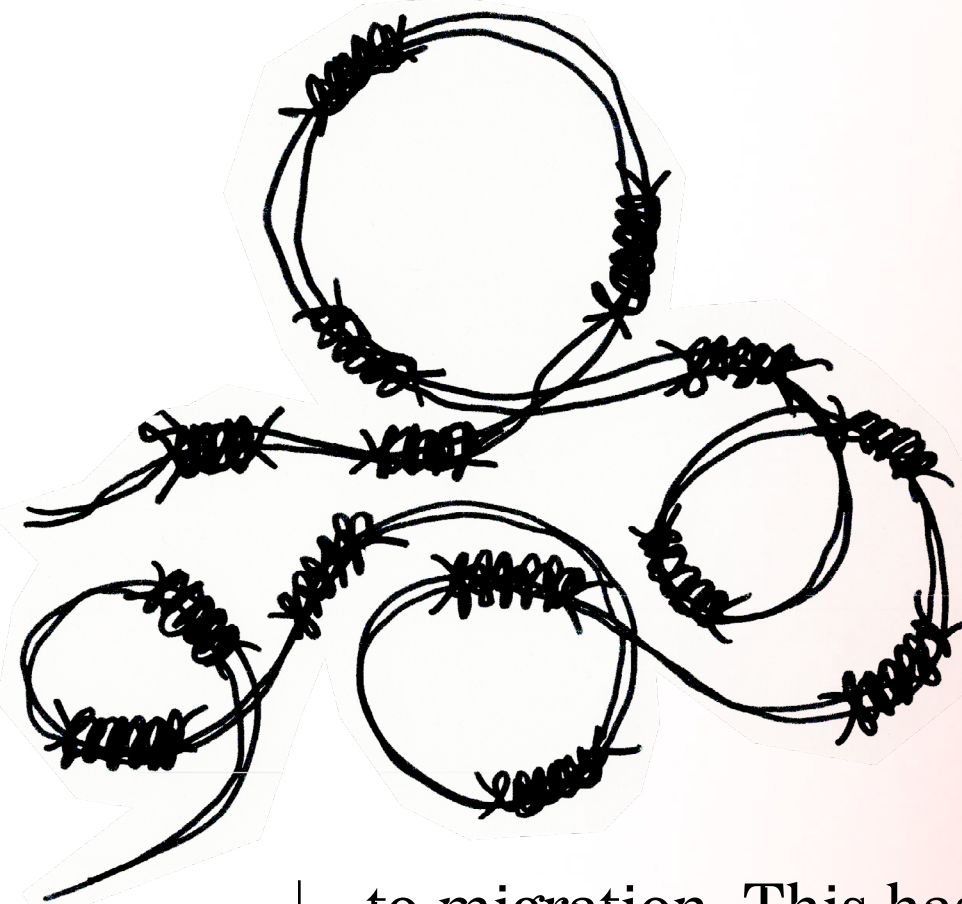
gation. While the exact number varied from year to year, on average, the top 1,000 “riskiest” recipients were selected for investigation. The system relies on the broad legal leeway authorities in the Netherlands are granted in the name of fighting welfare fraud, including the ability to process and 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”

“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”

Alyna Smith,
PICUM
2023

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”

“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 as 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 technolo-

gies 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 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 IN GREECE : AND HYPERION



Hyperion was described by the Hellenic Ministry 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 and simultaneous use of fingerprints), the monitoring of benefits per asylum seeker using an individual card (food, clothing supplies, etc.) and

movements between 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.”

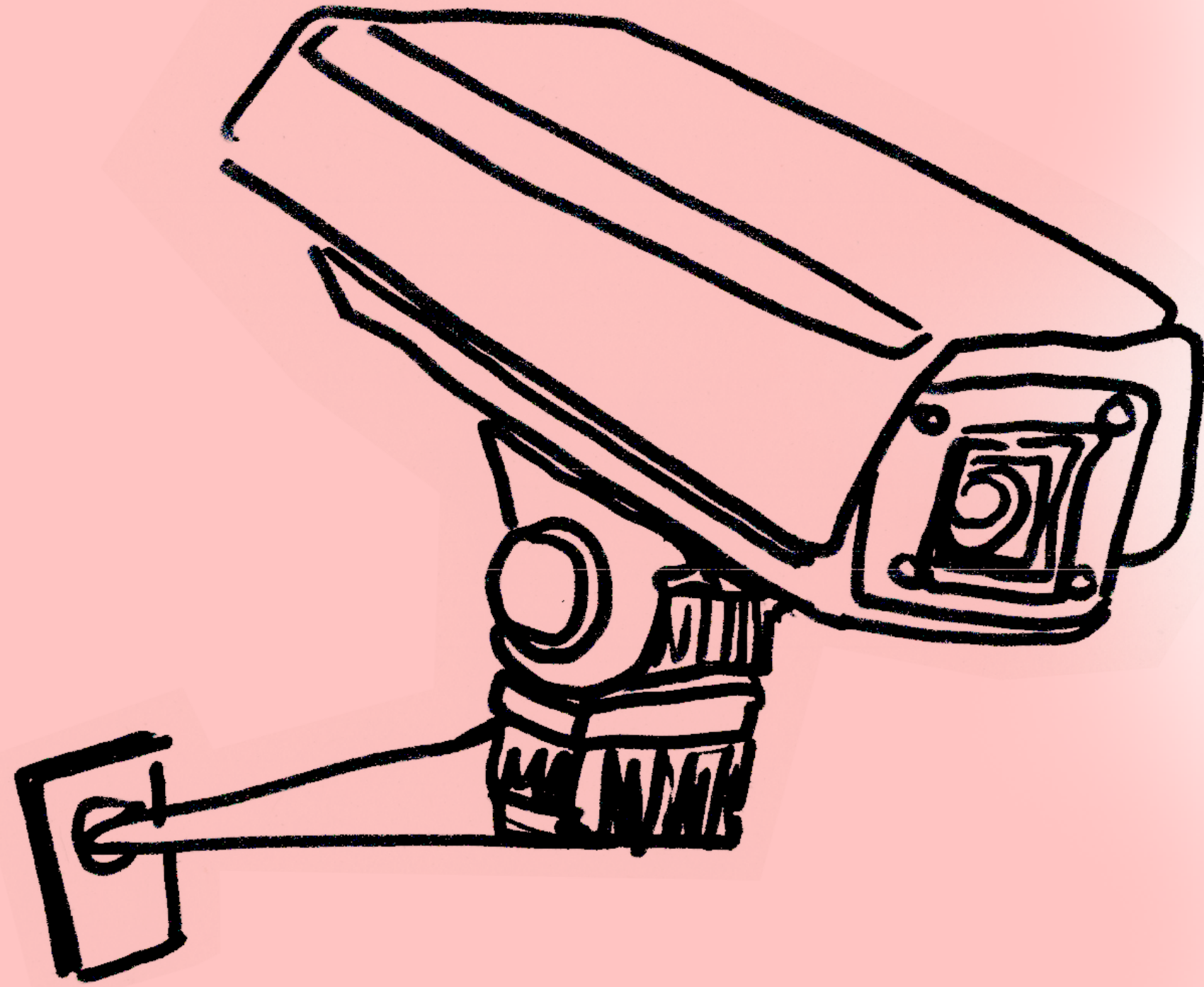
Centaurus was planned as “a digital system for managing electronic and physical security around and inside the facilities, using cameras and Artificial Intelligence Behavioral Analytics algorithms. It include(d) centralised management from the headquarters of the Ministry of Digital Governance and the 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 against 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

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”

“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”

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 (DFE, 2020).

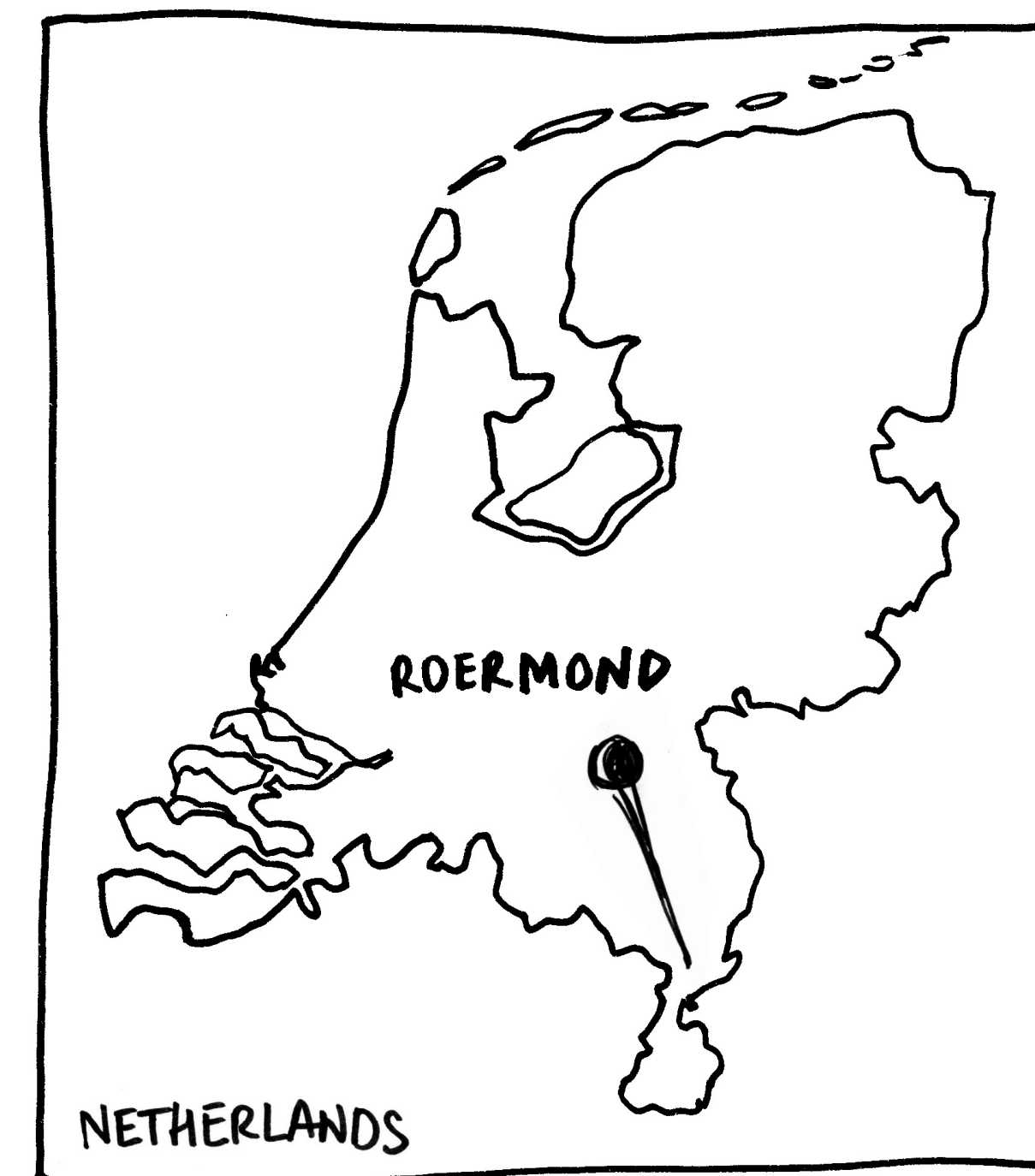
In France there is the increasing digital surveillance of public urban space, with tech imported from Israeli companies being used across the country and creating what has been referred to as “Smart Cities”, hundreds of millions of euros are invested into the development and implementation of softwares 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)

“Technoplice 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”

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 po-

lice 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 scale for which human surveillance only wouldn't be possible.

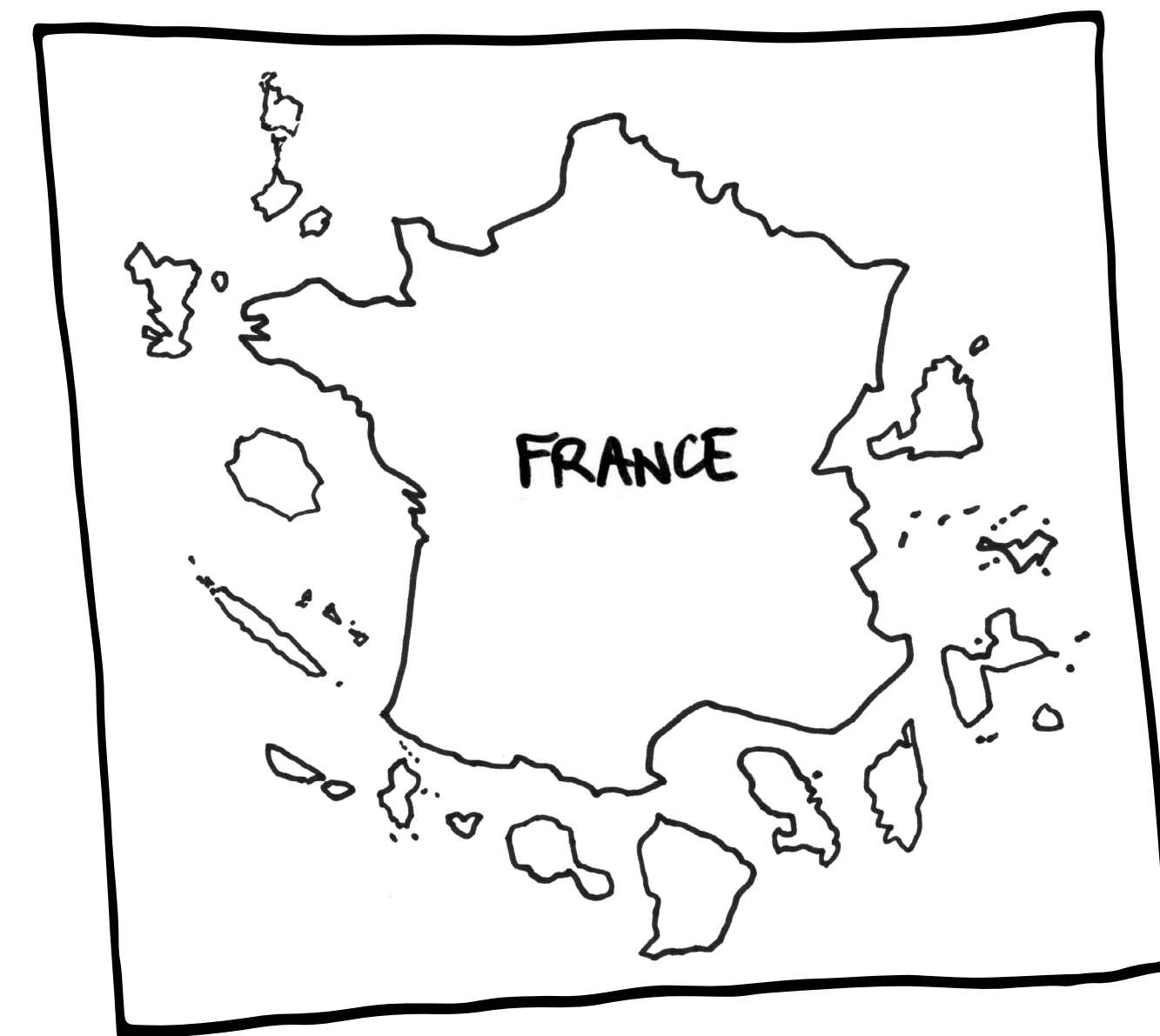
La Quadrature du Net defines algorithmic video surveillance as follow “the automation of the analysis of CCTV images thanks to a software that produce notifications when it detects an event that it has been trained to recognize. This analysis work was previously done by humans (municipal agents within 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 his-

tory 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

Online Activity That Causes Harm

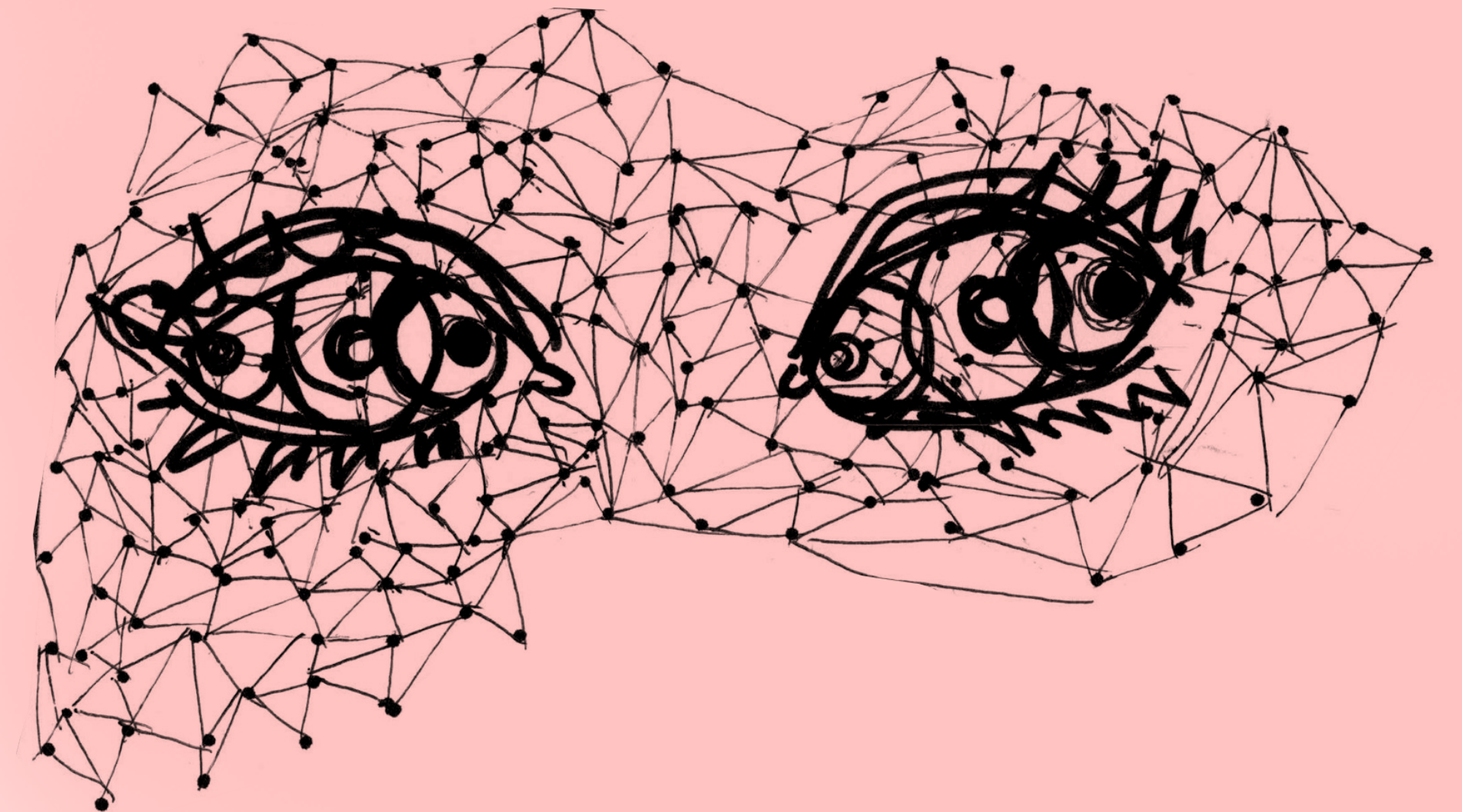
Hate speech is widely understood to be, offence discourse that targets a group or individual based on specific characteristics such as race, religious beliefs, or gender, which is used to cause harm, discriminate or incite hostility and violence (UN, 2023).

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 wi-

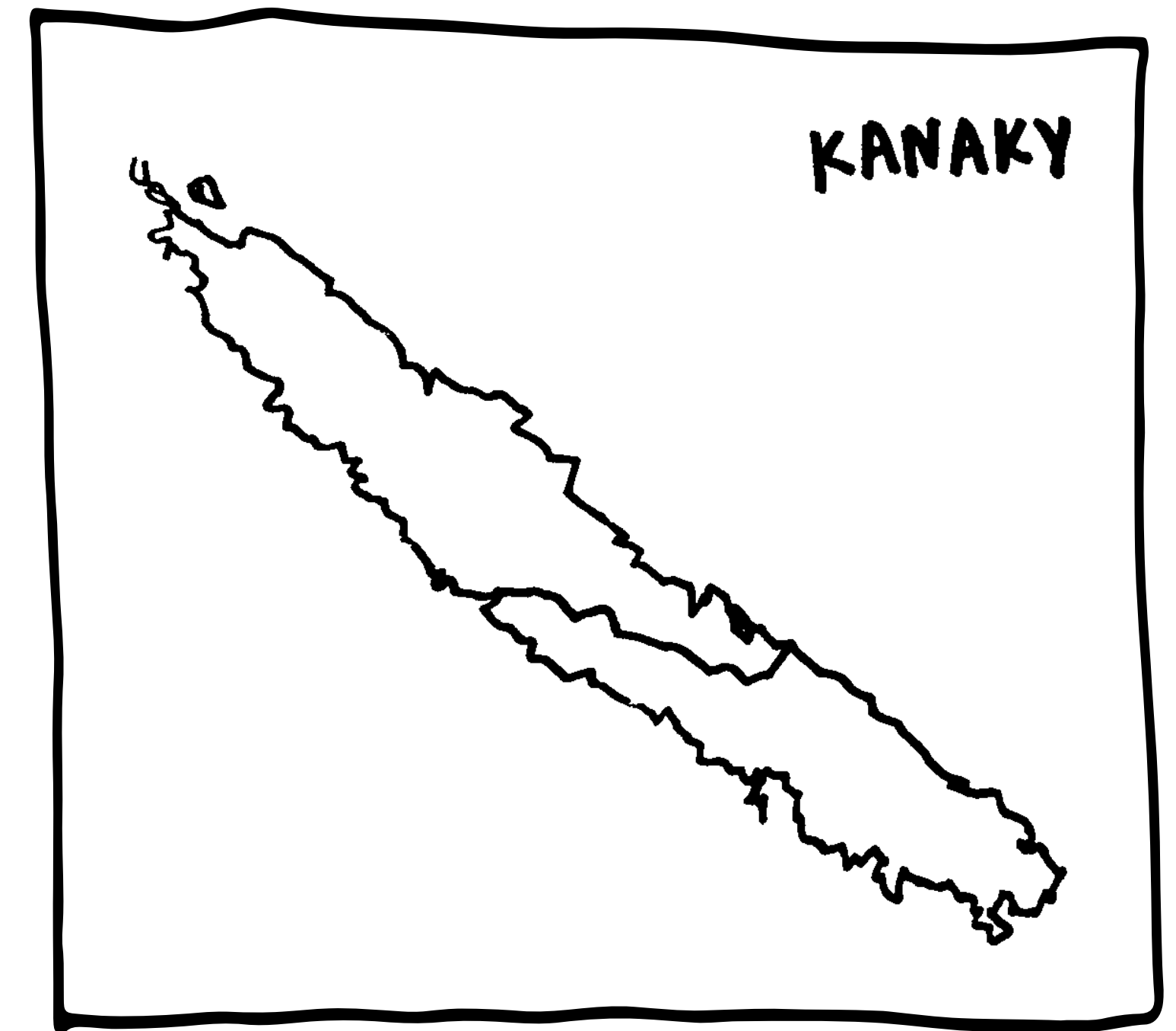
der lens around online activity which causes harm.

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).

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).



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 re-

ferendums 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.

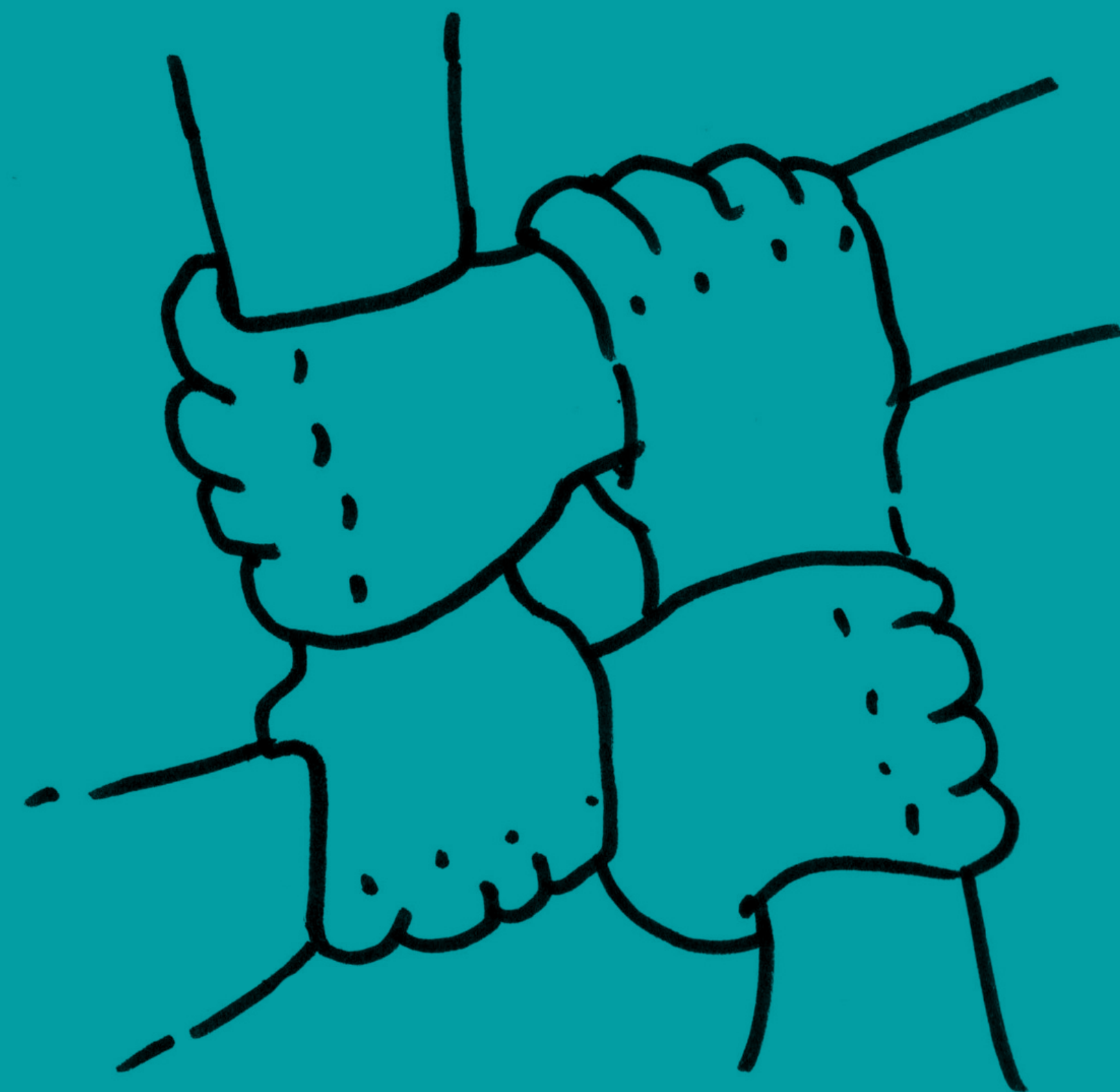
The TikTok block was implemented by the state-run Post and Telecommunication Service, the single

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.

TOOLS OF RESISTANCE



TOOLS OF RESISTANCE INTRODUCED...

In this section the tools that are introduced provide basic information about things we can do in our resistance against the harms of digital policing. The order in which the tools have been presented in the toolkit have been done so, because through our engagement with organisers, the tools have been used in a similar kind of order, with each one naturally folding into the next building blocks in a foundation to build community resistance from.

That said, you can of course pick and choose which way you use them, and

you may not want to use them all. We aren't going to tell you there is a wrong order, but we wanted to offer them in a way that allows you to see the potential of organising in a way that can build knowledge, community, capacity, resource, power and momentum.

It's also worth adding that you may find yourself working your way through and having to revisit one again, or consistently keep one or two ongoing. Resistance is not linear work, is happens in cycle, in tandem, and the urgency and/or need for different aspects

of the work ebbs and flows. You may find that you take a break or abandon something mid way to make room for something else. Its ok. Breathe. Recognise, we can't do everything, we can't be everywhere, but we can do what we can at the pace and in the places that are right, in that moment.

WE ASKED ORGANISERS:

What does resisting digital policing mean to you?



“For me it means developing strategies to avoid this policing, understanding the techniques and technologies to avoid it. In the same way, training ourselves in legal issues so that we know where the limits of the law are and can take advantage of them, just as those who violate our rights do.”

Sabrina Sanchez,
ESWA,
2023

“Resisting digital policing means centering marginalised communities’ needs in anything relating to policing. It means defunding the police as we know it today, and create instead ‘agents of care’ who work hand in hand with communities they have historically been harming”.

Oyidiya Oji,
European Network Against Racism,
2023

In the next section of the toolkit we will explore some of the tools we can use as part of our resistance efforts...

We learn **and BUILD** *from* *historical* **and GLOBAL** **RESISTANCE**

43

This toolkit recognises and pays homage to the radical histories and people of resistance that have been before us and paved the way for us to resist today. From the revolts against colonialism and slavery in Haiti, the Black power movement in the US, the end to apartheid in South Africa and the global Free Palestine, Sudan, Congo and Haiti movement.

In recent years we have seen Black Lives Matter uprisings, continued global resistance against oppressive systems of displacement, extraction, death and exploitation, national movements against oppressive states around borders and policing across Europe, and global movements against climate change.

We gain strength, knowledge, and encouragement by learning lessons from the experiences of those before us, resisted the oppressive power of the state, and found the courage, strength, and determination to fight back. We can use their experiences in our own methods of resistance and organising to build collective solidarity within communities which empower us towards liberation.

The efforts to resist policing institutions involves people from every corner of the globe. And many of us may feel intimidated, confused, and caught off guard by policing use

of tech. Of course we do, **the majority of us aren't tech experts.** But we will not allow this oppression to continue.

1. Empower: How we can empower ourselves with knowledge

2. Engage: How we can engage with others to build relationships and communities invested in resistance

3. Action: How we can take action to resist and fight against the digital policing of our communities

When we look at the tools in this tool kit, it may be that some people use them all, others may focus on particular ones, and some will use them in cycles, while many of us will swap and change between them depending on the need at the time, or even some or all of them in tandem. While there is an order to how they have been positioned in the kit, we do not believe you have to use them in one way, you know your communities, you know your experience, and you are specialists and experts in your own right. Find what is right for you, be willing to try, have the confidence to try and try again. The road of resistance is long, but there is hope, there is joy, and there is impact, and that is why we do what we do.

Raising awareness can take various forms, for instance:

- ▣ General conversation
- ▣ Campaign work in local areas
- ▣ National mobilisations

Raising awareness means that more people become aware. And the more people that are aware means that there are more people to join the resistance. Raising awareness can happen through 1 on 1 conversation, it can happen through meetings in local communities, it can happen through billboards and leaflets, through social media, through national news and journalistic reporting. The ability to raise awareness is vast, and it is key to bringing people into the fold.

44



“Raising awareness is key to building resistance, if people don’t know about the tech, or do know about it and are being harmed but feel isolated and alone, resistance is hard. But by speaking out about it, flyering, holding stalls, going into communities and creating space to talk about it we are able to build relationship and build resistance”

Catherine Barnett,
Freedom to Thrive
2023

Research means developing and deepening our understanding.

Knowledge gaps can become dead angles. And dead angles can cause us a myriad of obstruction and barriers.

Research can be/is key.
Academics can be allies.

Building relationships, or even utilising other people’s research (who we may not know) can supply us with the information we need to build resistance, raise awareness, or campaigns around.

When it comes to resistance,
KNOWLEDGE IS POWER.

Having information, knowledge, and understanding strengthens us.

EMPOWER 1/3



“We need to fill the knowledge gaps, we need more information about cases across the EU so that we can build a stronger movement by learning from others and sharing information with each other”

Oyidiya Oji,
European Network Against Racism
2023

Freedom of Information (FOIs) Requests

are a key tool to any and all type of social justice movement.

FOIs are used each and every single day; by the average person, academic researcher, and activist and campaign groups. All of which are striving for the same aim: to gain deeper understanding and knowledge.

FOIs allow us to request information from any public sector about information they hold.

The type of question posed is pertinent to the information that is provided.

Governments across Europe are obliged, by law, to respond, and supply information when FOIs are submitted.

There are “cost limits” attached to FOI requests, costs are based on the length of time it takes to gather the information. So if you need access to a lot of data it can make sense to make multiple specific requests but you can also ask them for guidance, when making your requests.

You can find a template on the next page/ in this toolkit to support you to make FOI requests...

FOIs can be done at a European Commission level, national government level, and local authority level. In some countries you are able to find information for previously supplied FOIs online and some authorities will not supply information that is already accessible in the public domain. In some countries you are also able to request information from individual organisations also. To find contact information search name of organisation and FOI on the internet.

EMPOWER
2/3

“I think that the lack of knowledge about the reach of these technologies is a big barrier to engaging in some sort of harm reduction. We really don’t know all the ways this [digital policing] can be harmful and without that, it is very difficult to identify the dangers”

FREEDOM OF INFORMATION REQUEST TEMPLATE



Dear [insert authority name],

I am writing to you under the [insert national government legislative act] to request information (from/regarding) [insert information here].

Please provide me with [details for relevant information requested and how it should be supplied].

If it is not possible for you to supply the information requested due to cost compliance, please provide advice and assistance as to how I can refine my request.

If you have further queries to my request please do not hesitate to contact me via the details provided.

I look forward to your response.

Yours sincerely,
[Insert name or group].

Things to think about:

- ☛ What information do you want?
- ☛ Why do you want it?
- ☛ Is the information already available?
- ☛ Which department/authority are you requesting information from?
- ☛ What is their contact email address/postal address?
- ☛ How much data/information are you requesting?
- ☛ Should you do multiple requests to increase likelihood of a successful request?
- ☛ Information that is deemed “sensitive” will probably not be provided.

CASE-STUDY: TOP400 IN THE NETHERLANDS



In the case of the Top400, most of the information known about how the system functions, using which criteria, were gathered via freedom of information requests.

“The documents consist of memos to the mayor of Amsterdam, steering

group and security triangle, three internal documents and emails, Top400 motoring reports and, finally, presentations. The documents span the years 2014 - 2019. Where needed, it draws on FOIA documents on the Top600. The more than 4,000 pages of FOI documents offer insights into

the origins, operations and conflicts of the Top400. What emerges is a picture of a top-down safety approach that allows a wide range of institutions to coordinate their actions in order to manage and control those minors and young adults whose behaviour is considered a nuisance to the city.

The voices, experiences, and needs of the minors and their families are completely missing from them”

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

COMMUNITY MAPPING TEMPLATE

WHO LIVES IN THE COMMUNITY?

WHAT CAN WE RECOGNISE TO BE DEMOGRAPHICS IN THE AREA?
(race, religion, age, income)

WHAT ISSUES ARE AFFECTING PEOPLE IN THE COMMUNITY?

WHO IS MOST AFFECTED?

WHAT LINKS TO THE COMMUNITY DO WE ALREADY HAVE?

WHO IS MOST AFFECTED?

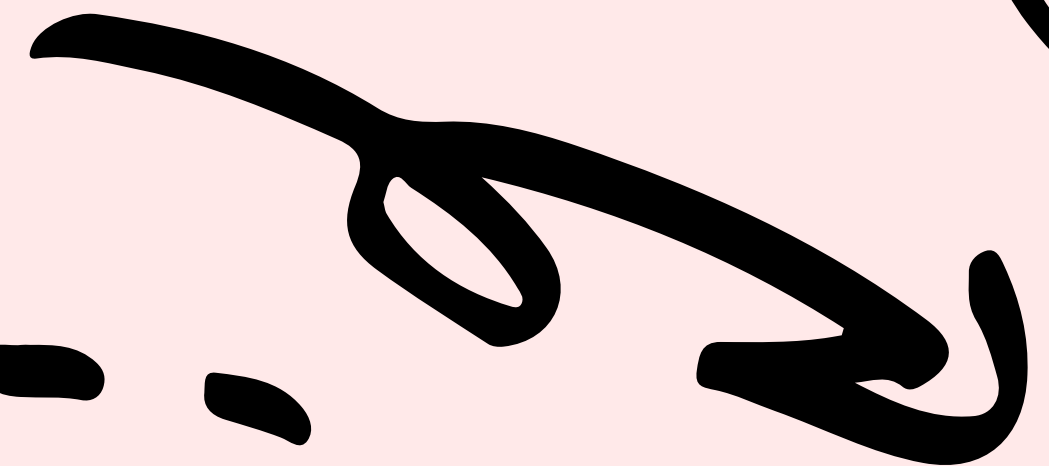
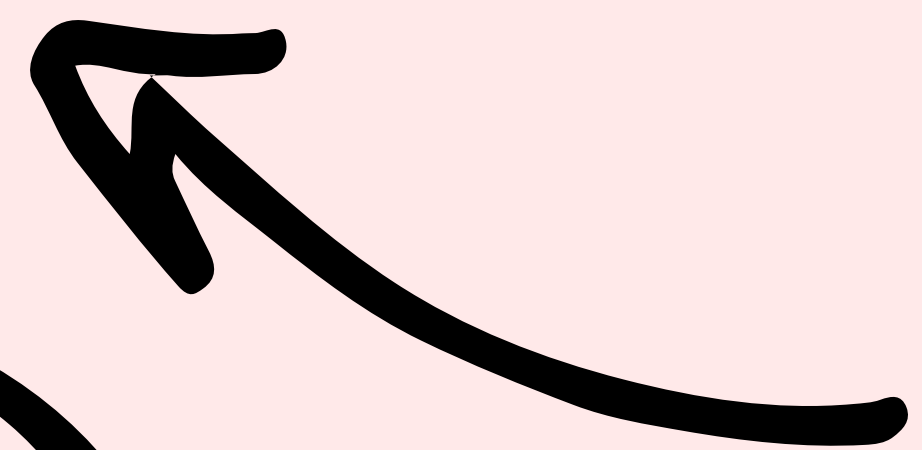
WHICH AREAS HAVE HIGH LEVELS OF FOOT TRAFFIC?

WHERE DO PEOPLE CONGREGATE?

WHAT SUPPORT SERVICES OR MECHANISMS ARE BASED IN THE COMMUNITY?

WHAT IS THE POLITICAL PARTY IN POSITION?

WHAT RESISTANCE WORK TAKING PLACE LOCALLY?



When building resistance at a community level, knowing and understanding what the community looks, feels like, is what allows us to identify who we need to work with, how we are going to make contact, how we build relationships, how we support ongoing work, and how we build resistance in the community.

Part of building resistance is also understanding when, where, why, and how harm is taking place, specifically in this case, when, where, why, and how digital policing is taking place.

Community mapping is a tool which can unlock some of this information, and guide us to make and develop plans.

To do this work, is to find answers to questions that deepen understanding and support strategy and implementation.

COMMUNITY MAPPING TEMPLATE

PRINTABLE TEMPLATE ON THE NEXT PAGE!

WHO LIVES IN THE COMMUNITY?

WHERE DO PEOPLE CONGREGATE?

WHAT ISSUES ARE AFFECTING PEOPLE IN THE COMMUNITY?

WHAT CAN WE RECOGNISE TO BE DEMOGRAPHICS IN THE AREA?
(race, religion, age, income)

WHICH AREAS HAVE HIGH LEVELS OF FOOT TRAFFIC?

WHO IS MOST AFFECTED?

WHAT CAN WE RECOGNISE TO BE DEMOGRAPHICS IN THE AREA?
(race, religion, age, income)

WHICH AREAS HAVE HIGH LEVELS OF FOOT TRAFFIC?

WHAT SUPPORT SERVICES OR MECHANISMS ARE BASED IN THE COMMUNITY?
(race, religion, age, income)

WHAT LINKS TO THE COMMUNITY DO WE ALREADY HAVE?
(race, religion, age, income)

WHAT IS THE POLITICAL PARTY IN POSITION?

WHAT RESISTANCE WORK TAKING PLACE LOCALLY?

There is a basic resistance community mapping template which gives an idea of how you can map your community.

This template could be used at an extremely local level, like a housing estate, but also used for a town, city, country....

EMPOWER 3/3

COMMUNITY MAPPING TEMPLATE

WHO LIVES IN THE COMMUNITY?

WHERE DO PEOPLE CONGREGATE?

WHAT ISSUES ARE AFFECTING PEOPLE IN THE COMMUNITY?

WHAT CAN WE RECOGNISE TO BE DEMOGRAPHICS IN THE AREA?
(race, religion, age, income)

WHICH AREAS HAVE HIGH LEVELS OF FOOT TRAFFIC?

WHO IS MOST AFFECTED?

WHAT CAN WE RECOGNISE TO BE DEMOGRAPHICS IN THE AREA?
(race, religion, age, income)

WHICH AREAS HAVE HIGH LEVELS OF FOOT TRAFFIC?

WHAT SUPPORT SERVICES OR MECHANISMS ARE BASED IN THE COMMUNITY?
(race, religion, age, income)

WHAT LINKS TO THE COMMUNITY DO WE ALREADY HAVE?
(race, religion, age, income)

WHAT IS THE POLITICAL PARTY IN POSITION?

WHAT RESISTANCE WORK TAKING PLACE LOCALLY?

ENGAGE 1/6

Oyidiya Oji,
European Network
Against Racism
2023



Outreach is a tool which is key to resistance and campaign work.


The power and reach of resistance and campaigning is often reliant on having people engaged and empowered to act. Capacity is consistently named as a barrier of resistance work.

Outreach allows us to connect with people.

Outreach is about reaching people, raising awareness, and inviting them in. And so it is a key tool for us to use and utilise.

Using the community mapping tool allows us to identify the places where outreach can be the most successful and have the most positive impact.

Any and all outreach must be respectful, flexible, welcoming, accessible and accommodating!



Outreach work has to be approached sensitively, as with any relationship building. Outreach should not place responsibility or expectation on community.

Building relationships is a key tool to strengthen our efforts to resist digital policing and mitigate the harm that it perpetuates.

We must dedicate the time and effort that relationship building deserves and these relationships should have benefit to everyone, but prioritise those who are most affected by the harms of digital policing.

Transparent, cohesive, and accountable relationships form the backbone of strong community resistance work.

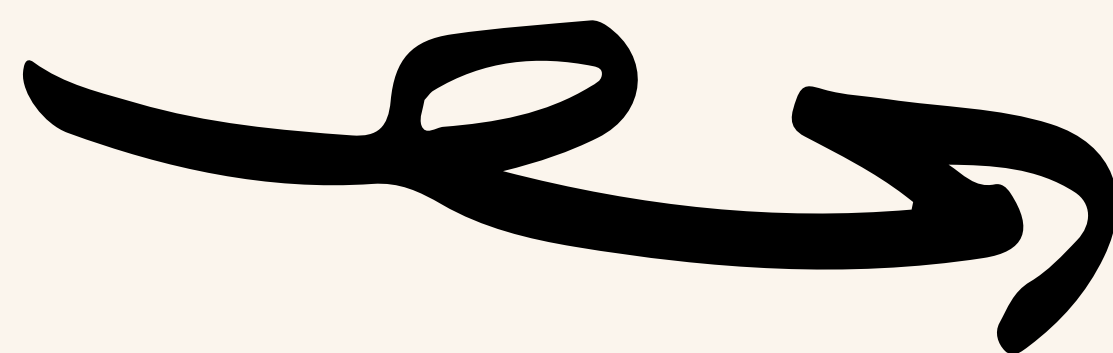
To this we utilise the tools we have already described, accessible language, time, mapping, and centering the lives of those most marginalised.

Our principles and values should be clear and steadfast and provide grounding for building together.

ENGAGE

3/6

MEET PEOPLE WHERE THEY'RE AT!



“Language is so important, it can be a barrier or a tool. Our language has to be accessible, and we need to find a language that is accessible to everyone who involved in resisting digital policing”

Useful language needs to be just that: **USEFUL!**

The language around digital policing technology is linked to who works on it. And the majority of people who are fluent in the language around it at the moment are tech and legal experts!

So in order to ensure that more people are join resisting digital policing we need to ensure that more people are able to understand it!

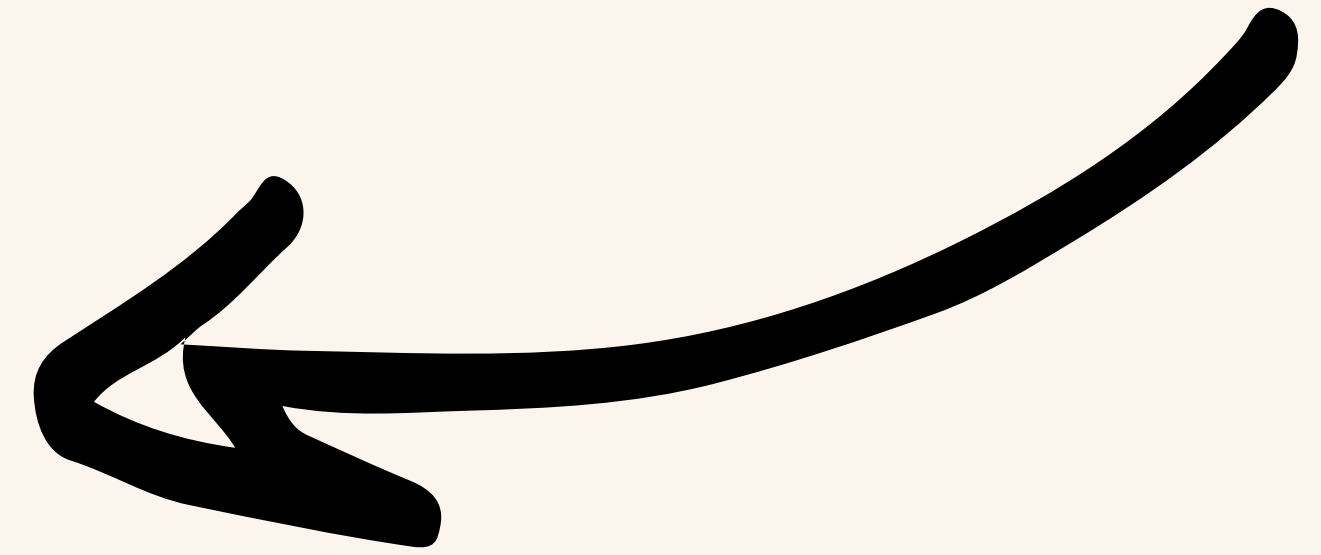
Not only can this mean preventing the use of jargon, it means simplifying language and centring the effects and consequences rather than the functioning of the technologies centring language to be useful instead of fulfilling academical requirements when talking in community will allow different people from different lived experiences, groups, expertise to communicate with each other so that we are able to build resistance as a collective of people.

ENGAGE
4/6

Oyidiya Oji,
European Network
Against Racism
2023

54

“It is so difficult for affected community members, who are already marginalised, to speak up about their experiences of being victims of digital policing. Not only is language a barrier because tech language is not something people are familiar with but it also hold a danger of retraumatizing people”



Our activism, resistance, and collective power-building must be rooted in foundations which centre, prioritise and uplift the experience and voices of those most harmed or likely to be harmed by digital policing.

It sounds like a simple thing, and in some ways it is, but it also **takes time, collaboration, and needs flexibility, care and empathy.**

It also means unlearning habits some of us have picked up. **There is no room**

for saviourism in resistance work. And being extractive does not enable us reaching circumstances of equity.

It also takes balance, many people engaged in resistance work who are also affected and harmed, find themselves in a cycle of survival, resistance and building. Allowances have to be made for this. The survival work is crucial to resistance, and the building is key to survival and resistance.

ENGAGE 5/6



TRAVEL SUPPORT	
COSTS	
VENUE	
FOOD/ REFRESHMENTS	
LEAFLETS	
BANNER MAKING	
SUBSCRIPTIONS	
DIRECT ACTION	

Resistance work costs a lot. It costs time, it costs energy, it costs emotion, it costs money. And the more people you talk to, the more ideas and inspirations happens and creates conversations for strategic planning to embark in resistance.

It makes sense to recognise budgeting and fundraising as tools in our resistance because for too long this has been shield away from and the work can become too arduous or can even get to stages where we have the ideas and the plans but lack the ability to move forward with them.

We shouldn't shy away or be ashamed of needing money and resources to support our work, afterall we are going up against some of the most well funded institutions in the world.

Many of us have an ability to make a little go a long way, its a mechanism of survival in our personal lives. And we can apply those skills in our resistance work where we need to but we can also be honest about the costs of this work so that we can use that information to budget, fundraise and identify places to draw resource from.

ENGAGE 6/6

The power of dialogue should not be ignored or denied. In resistance work, dialogue is crucial to success!

To resist digital policing we have to be able to openly talk about what is happening, where harm is happening, what the impacts are.

We also need to talk how people feel, what people are doing to survive or fight back, what resources people have or need, strategies that they have or are planning and building around.

Dialogue is an art form, an art form which we should practice, maintain, develop, and most importantly, utilise! 121 conversation, group conversation, panelled discussions, online meetings, research, campaigning, you name it, dialogue is there and it is key!



Sabrina Sanchez,
ESWA
2023

When we build strong relationships with people and groups it gives us access to more information, more perspectives, more experience, more expertise, and more resources.

Our capacity increases by building relationships. And a key outcome that we should think about when building relationships is what we bring to the table, what we are lacking, and what we need. Relationship allows us to discuss these things and identify who is able to share what they have whether that it is information and/or resource.

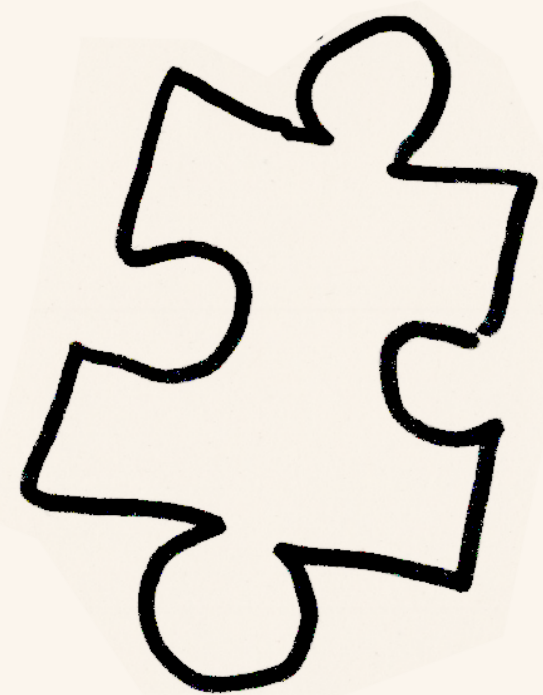
Sharing our information and resources empowers resistance, it empowers the movement to resist digital policing.



Oyidiya Oji,
European Network Against Racism
2023

ACTION

1/4



Political education in resistance work is little “p”, and rather than it being focused on parliamentary politics, it is education that aims to support and further collective solidarity and liberation.

Drawing on past, ideologies, creating space for discussion and strategizing, political education creates accessible space that deviates from the mainstream narrative and empowers people, building knowledge and building power.

Political education is a tool that we can utilise to broaden and deepen people’s understanding of the oppression and harm that individuals and communities are facing.

It allows us to understand the powers and systems which facilitate the harm and violence from digital policing, and the ideology that is driving it.

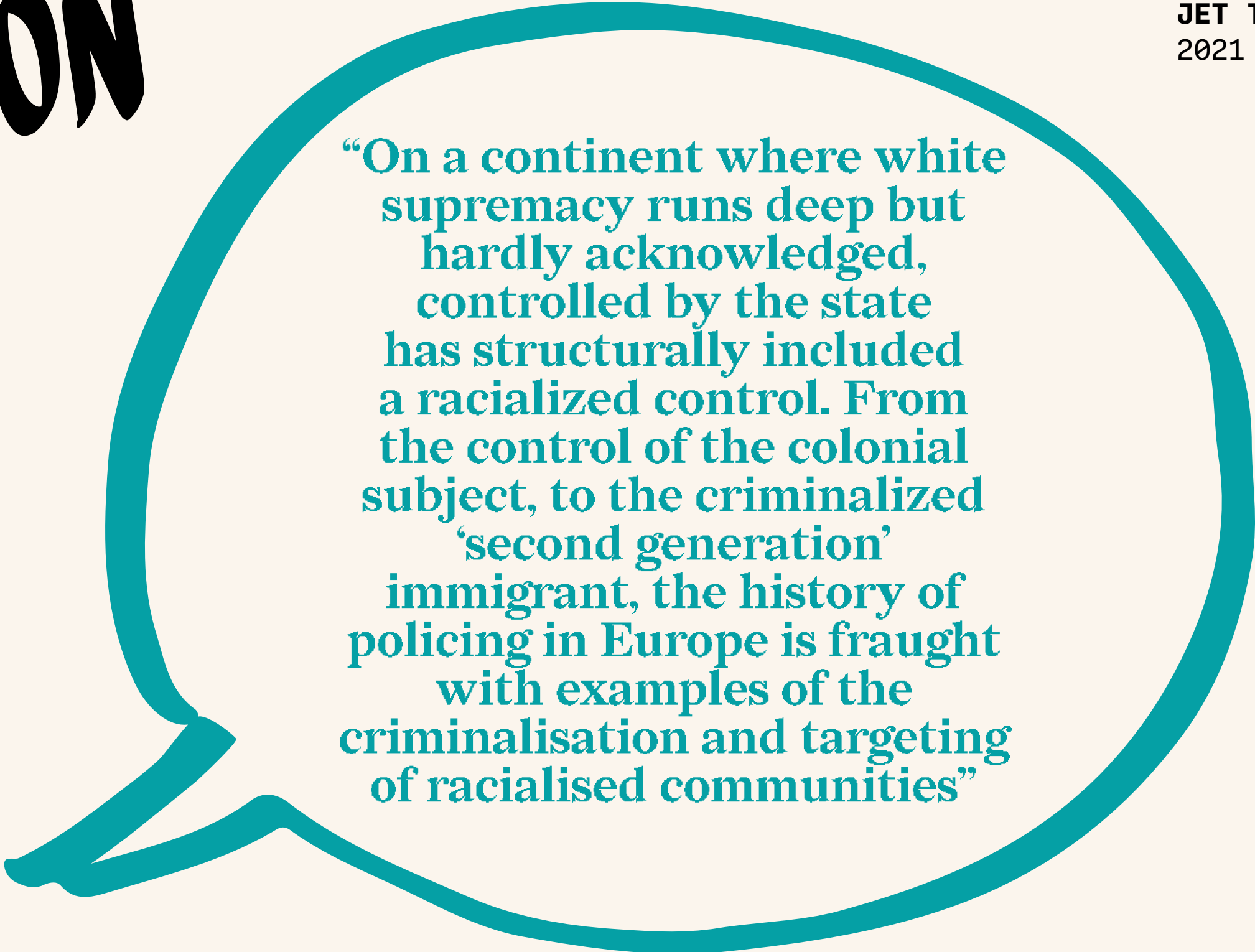
Building our political education frameworks around social

justice allows us to raise collective consciousness, develop empathy, and enable us to identify ways which we can build relationships, coalition, allyship.

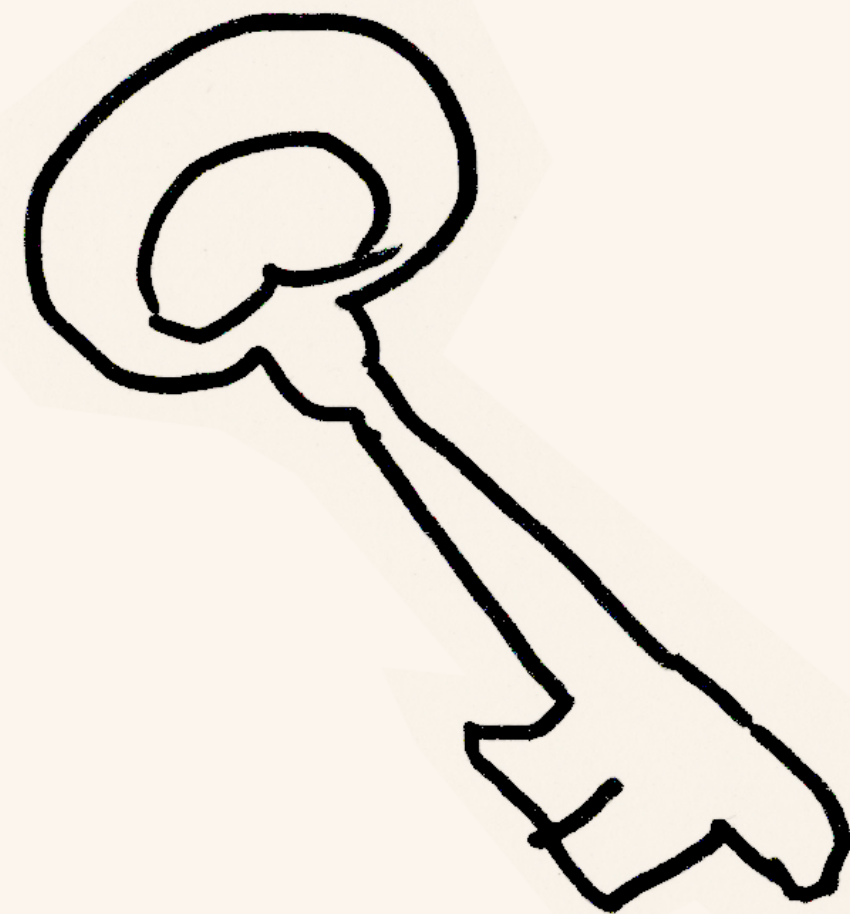
Political education also allows us the space to listen and learn from people’s lived experience, understanding the impacts, and how those affected would like to be supported to prevent, mitigate, and heal from harm.

ACTION 2/4

Esra Ozkan & Sanne Stevens,
JET Table
2021



“On a continent where white supremacy runs deep but hardly acknowledged, controlled by the state has structurally included a racialized control. From the control of the colonial subject, to the criminalized ‘second generation’ immigrant, the history of policing in Europe is fraught with examples of the criminalisation and targeting of racialised communities”



Just as we map communities, we need to map the use of digital policing technologies!

Mapping the use of the tech allows us to identify who is using it, how it is being used, where it is being used, who is affected by its use, and what the impacts of its use are.

This information and understanding is key for us to plan and strategize around because it gives us insight into who we need to build relationships with, what support and resources we need,

areas of resistance work that needs to be prioritised.

It also allows us to understand where our knowledge gaps are, and where we need to do more research, to gain more understanding.

Mapping the technology also allows us to identify where we need to outreach, where we need to think about implementing protections, and how we can engage in harm reduction.

WHAT DIGITAL POLICING TECHNOLOGY IS IMPACTING COMMUNITY?

IS THERE DIGITAL POLICING TECHNOLOGY PHYSICALLY PRESENT IN THE COMMUNITY?
(ie, in public areas and what is the purpose of the technologies?)

HOW IS TECHNOLOGY BEING USED TO DIGITALLY POLICE INDIVIDUALS?

WHO IS BEING IMPACTED BY DIGITAL POLICING TECHNOLOGY?

WHERE IS THE TECHNOLOGY IN PUBLIC PLACES?
(you could use an actual geographical map for this)

WHICH AGENCIES ARE UTILISING TECHNOLOGY TO POLICE INDIVIDUALS?

TECHNOLOGY MAPPING TEMPLATE

WHAT AGENCIES ARE USING THE TECHNOLOGY?

WHO IS MOST AFFECTED BY THE PRESENCE OF THIS TECHNOLOGY?

HOW WIDESPREAD IS THE IMPLEMENTATION OF THE TECHNOLOGY AND HOW LONG HAS IT BEEN PRESENT?

WHAT ARE THE IMPACTS OF THE TECHNOLOGIES PRESENCE ON THE COMMUNITY?

WHAT ARE THE IMPACTS OF THE TECHNOLOGIES BEING USED?

TECHNOLOGY MAPPING TEMPLATE

**WHAT DIGITAL
POLICING TECHNOLOGY
IS IMPACTING
COMMUNITY?**

**IS THERE DIGITAL POLICING
TECHNOLOGY PHYSICALLY
PRESENT IN THE COMMUNITY?**
(ie, in public areas and what is the purpose
of the technologies?)

**HOW IS TECHNOLOGY BEING USED
TO DIGITALLY POLICE INDIVIDUALS?**

**WHO IS BEING IMPACTED
BY DIGITAL POLICING
TECHNOLOGY?**

**WHERE IS THE TECHNOLOGY
IN PUBLIC PLACES?**
(you could use an actual geographical map for this)

**WHICH AGENCIES ARE UTILISING
TECHNOLOGY TO POLICE INDIVIDUALS?**

**WHAT AGENCIES ARE USING
THE TECHNOLOGY?**

**WHO IS MOST AFFECTED
BY THE PRESENCE
OF THIS TECHNOLOGY?**

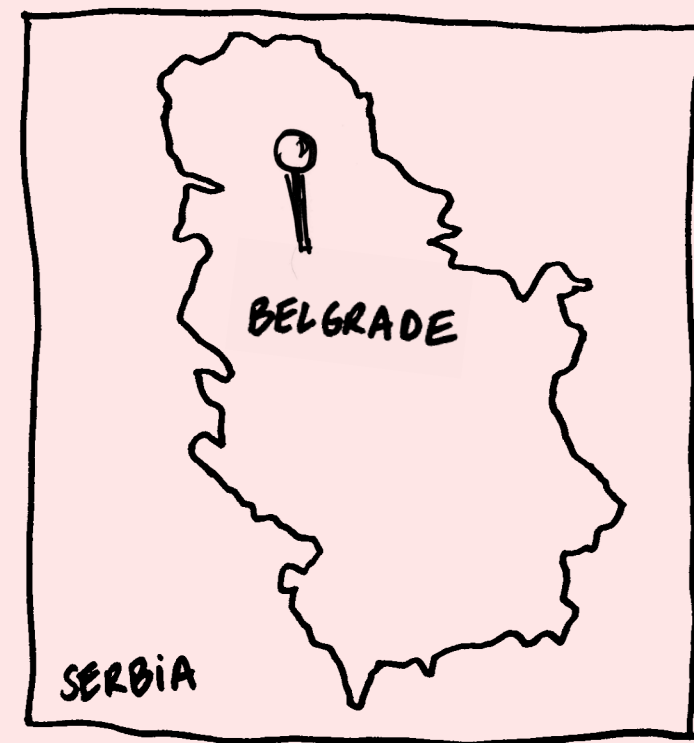
**HOW WIDESPREAD IS THE
IMPLEMENTATION OF THE TECHNOLOGY
AND HOW LONG HAS IT BEEN PRESENT?**

**WHAT ARE THE IMPACTS
OF THE TECHNOLOGIES
PRESENCE ON THE
COMMUNITY?**

**WHAT ARE THE IMPACTS
OF THE TECHNOLOGIES
BEING USED?**

PRINT ME!

CASE STUDY: HILJADE KAMERAS IN SERBIA



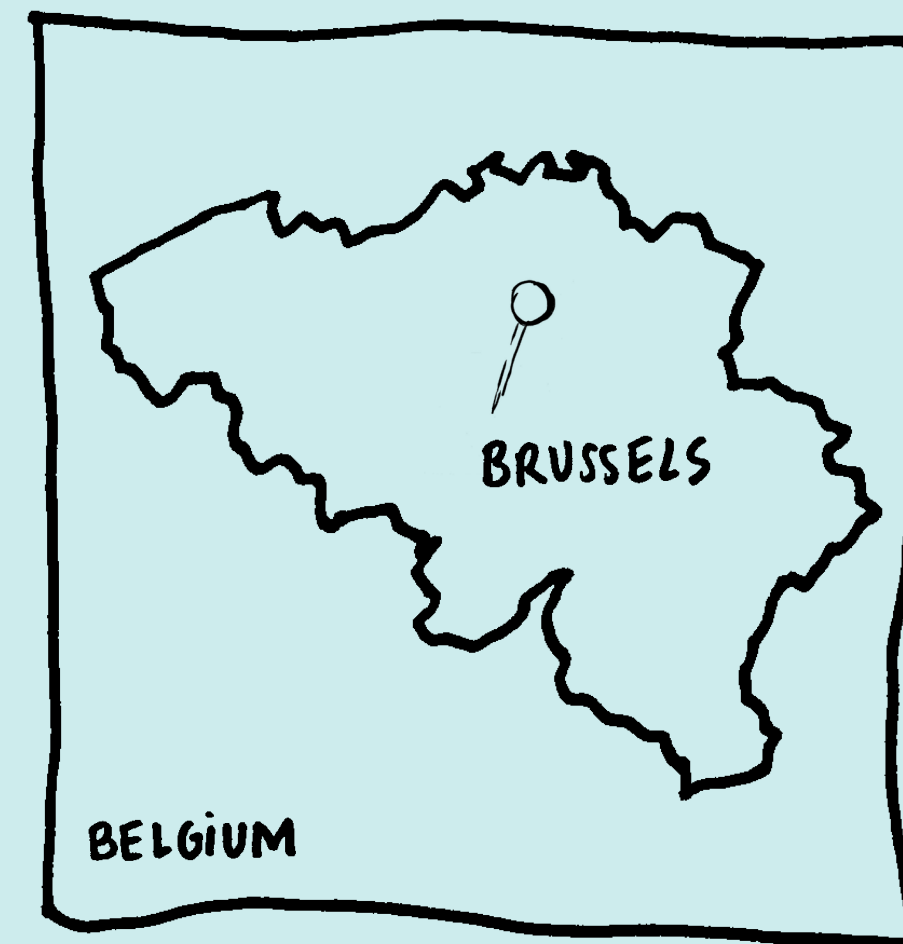
“The Government of Serbia in cooperation with Huawei has been actively working on the implementation of the ‘Safe City’ project in Belgrade. This project involves the installation of thousands of smart surveillance cameras with object and face recognition features. The procurement also involves an artificial intelligence system used for the analytics of the feed captured with these cameras.

A civic initiative, [#hiljadekamera](#) [Thousands of Cameras] is tracking the development of the mass surveillance system in Belgrade and has so far collected and verified data on 689 facial recognition cameras across the city. Composed of concerned citizens, experts and digital rights organisations,

has been vocal about the deterioration of privacy as a result of this project for over a year. The website with the map showing locations of smart cameras [hiljade.kamera.rs](#) was launched in mid-May (2020), together with social media accounts. In the first two months of this crowdsourcing action, the citizen map revealed twice as many smart cameras than there are on the official police list. Major discrepancies are noted in Novi Beograd, Zvezdara, Stari Grad, but also in other municipalities of Belgrade.”

■ SHARE Foundation presents [#hiljadekamera](#): A documentary on biometric mass surveillance. [online] EDRi website, consulted in June 2024.

CASE STUDY: CARTO.TECHNOPOLICE IN BELGIUM



The Belgium section of the Techno-police initiatives created a guide to map of cameras in your community available in French named “Guide de cartographie du contrôle social”.

They themselves did one concerning Brussels, available at [carto.techno-police.be/](#).

ACTION 3/4

Campaigning is a key tool of resistance.

Simply defined, to campaign is to work together in a active and organised way towards a specific goal or outcome.

Campaigns allow us to raise awareness, raise consciousness, share information, share resources, build relationships, gain information, apply pressure, and make demands.

We are surrounded by campaigns from marketing campaigns to get us to buy something, to political campaigns to get us to vote for a particular party.

An effective resistance campaign utilises all of the tools in this kit!

Direct Action identifies a target that enables organisers to assert pressure.

For example the Palestine Action group in the U.K. has focused their organising efforts on targeting weapon developers and investors who enable the occupation of Palestine. They do this consistently and assertively, to disrupt day to day operations around the UK, and since recently around the world.

Resistance is a natural by product of oppression, and Direct Action has always played a key role in resistance work.

In simple terms Direct Action is using public forms of protest to reach demands, rather than engaging in negotiation.

Direct Action can take many different forms, mass mobilisation marches, strikes, banner drops, building occupations, artistic outputs, road blockades, covering camera lens, the list of potential goes on and on.

Direct Action has been used throughout history and across movements with some tactics being long term plans, and others short term, but the effects that they have had can not be denied, it is a powerful tool of resistance.



Campaigns don't take one specific form but rather speak to being able to adopt a specific output to reach an audience, raise awareness, build power, create new things, and make demands. They can take place in a small local community, have a national outlook, or take place online.

ACTION 4/4



Some hints and tips:

- ☞ Use encrypted apps like **Signal** or **Jitsii** to communicate
- ☞ **Rise Up pads** are open source documents that should be preferred to **Google Docs** and **One Drive**
- ☞ Use pseudonyms in organising chats
- ☞ Don't post anything which can be used to criminalise people online



While this whole toolkit is about digital policing and the harms of the use of technology against communities, we as people resisting its use are in many ways very much dependant and engaged in the use of technologies ourselves.

We know that our use of technology can be used against us, that it can be monitored, that it can be used as evidence against us.

With that in mind it is important for us to think about the software we use and prioritise using software which provides some safety protections to allow us to communicate with each other.

We know that the state has backdoors into the Big Tech giants such as Google, and that there is no such thing as 100% secure but we can try our best to keep ourselves safe.

While organisers often face the threats of the criminal (in)justice systems, and

we are working towards the day that these harmful systems cease to exist, while they do we must recognise that sometimes, not only will they be used against us, we may also utilise them to further our cause.

Lawyering can be used as a tool where legal experts can support campaign work to take strategic litigation against the state.

There are specialist lawyers who work to support people involved in resistance work and racial justice work around the world, and they have been key in overturning, undoing, and changing harmful legislation.

Forming relationships with lawyers who understanding the importance of working from the lived experience of marginalised people and use this to inform their work and engage is strategic litigation is a powerful tool of resistance.

This toolkit offers an introduction to some of the main tools of resistance we can use to resist digital policing, as individuals, and as community organisers.

We don't have all the answers, and we aren't saying any of this work is easy. But what we do hope is that it gives people some starting off points on how we can utilise these different mechanisms to

build in our communities. One thing that we know is that our resistance work is successful when we are working from the position of achieving liberation for those most marginalised, and when we are doing so in solidarity with others, and building with others can allow us to build movements which change the world as we know it.

**Community Experience,
Community Resistance,
and Community Organising,
can lead us to building
sustainable Community
Centred Movements.**

In the next and final part of the toolkit let's see how we can build resistance on a larger scale by building a movement to resist digital policing...



BUILDING
A MOVEMENT



**“Building a movement
is a culmination of all
of our resistance efforts.
Building a movement
revolves around
relationships, and strong
relationships take
time to build.”**

What is a social justice movement?

Social justice is the view that everyone deserves equal economic, political and social rights, protections and opportunities. In its plainest form, a movement is a group of people working together for a common social, political or cultural goal. Movements can focus on an injustice, an opportunity for change or even a promotion of a theory or concept.

Why is a social justice movement an important part of resisting digital policing?

Resisting digital policing aims to allow us to protect ourselves and mitigate the harm that digital policing causes to our communities, until the day that we can abolish these systems of harm all together.

Building and being part of a movement strengthens our ability to resist digital policing. Just as the reach of policing spans borders, so too must our solidarity and action.

To build a movement we work together not as individuals and groups, within our own areas of specialism, interest, or strength, but as a collective, a coalition, a unified people, towards the same goal. Movement building is a key part of mass mobilisation which works to strengthen and advance our resistance work.

Solidarity and resistance is an active and continuous journey, that ebbs and flows, it twists and turns but it is active and continuous, and the movement is how we refresh, recharge, reach our goals.

In this toolkit, we have talked about tools of resistance, just as resistance work takes time, care, and dedication, so too does building a movement. While we generally engage in resistance work as individual organisations engaged in specific resistance work, building a movement means working together with others who are also working towards the same goals.

Movement building takes more time, more resources, more reach, and that means we need more people. Our strength is in our unity, and our unity comes from relationships. So let's have a look at some of the ways that we can do this work...

STRATEGIC COALITIONS IN LOCALISED ORGANISING

While a lot of resistance work happens on a local basis, and of course is done strategically, many resistance groups can find their efforts, (rightly) focused on the immediate issues that their communities are facing. But this can often mean that there are many different groups working on specific issues in a particular area. And sometimes this work can become siloed.

Strategic Coalitions in Localised Organising allows us to pull away from siloed organising and work together in coalition.

Building local coalitions allows us to work together, build solidarity, raise awareness, and strengthen our efforts. Coalitions allow us to work in our priority areas towards a collective goal. To build strong local links to build momentum, and movements can play a key part in our success.

To build a strong coalition it is important to ensure that those involved agree on values, and take time to build relationships, and understand each others work. When you do this you are able to then hold strategic conversations and make non-hierarchical decisions on how you can work together towards the same collective goal as well as work in solidarity by sharing resources, engaging in knowledge sharing and building collective power as part of a movement.



NATIONAL COALITION BUILDING

National coalitions take time, energy, resource, dedication, a lot of dialogue and a lot of work. And while we know that when engaged in this survival work we do, we may have less time for building long term, widespread relationships, we believe that they are a powerful tool and asset that cannot be overlooked.

Coalitions allow us to bring in people from across the different sectors, with different experiences, different interests, different specialisms, and create the perfect place for people to draw on these to work together towards the same goal and in support of each other. They allow us to hold more power, and apply more pressure, they allow us to share resources, they allow us to mobilise on a mass scale, and they allow us to embed practices of care by having more people to share the labour.

While the state focuses on dividing us, and weakening our resolve, national networks allow us to unify on a larger, longer, and stronger scale.

National coalition building sounds exactly like what it says on the tin, **building relationships to work in coalition on a national scale towards the same collective goal(s)**.

National coalitions can be integral to movement building, because what we know about digital policing, is that not only is it affecting people on their

door steps, it is affecting people on their doorsteps everywhere.

Resisting digital policing affects us as individuals, as communities and as a populations as a whole, and so building coalitions that work to resist digital policing on a national scale is a strong way to build momentum and collective power.

Like with coalition building and local community organising, shared values, shared principles, shared aims and goals, are key, and so is communication, trust, and relationship.

INTERNATIONAL COALITIONS

International coalitions can start from personal relationships, they can start from solidarity actions, they can blossom from social media campaigns, and they can be thrust forward following emergencies that need response. How they start, is less important than how they are built- the same tactics and tools apply, aligned values and principles, agreed goals, a desire to be in mutually respecting and trusting relationship, and active solidarity. These are the simple foundations that can create sparks that light fires which change lives, and legislation. Which empower us, create safer communities, change political landscapes, and allow us to thrive.

Dream with us friend, and take that step to build global resistance and liberation.

Here is it again, that word, coalition, and that's because we truly believe there is so much to be gained from the more people we have in relationship.

The policing of our communities is global, they are marketed on a global scale, and **so our resistance must also be global.**

We only have things to gain by working on an international level with those who are also working to dismantle the systems of policing.

International Coalitions allows us to learn, to exchange, to build, to dream, to understand, to empathise, to be in active solidarity, and the beauty and potential of the

power of an international movement is limitless.

These things of course take time, and may start small, but just as we aim to dismantle the systems of oppression brick by brick, so to will we build new ways of the world which allow us to engulf ourselves in systems of love and liberation.

WHAT KIND OF PEOPLE OR GROUPS ARE ENGAGED IN SIMILAR WORK?

WHERE IS THE WORK TAKING PLACE?

WHAT SPECIALISM ARE NEEDED TO BUILD A COLLECTIVE MOVEMENT?

WHAT VALUES AND PRINCIPLES MUST GROUPS AND PEOPLE BE ALIGNED WITH?

WHAT SKILLS GAPS DO WE HOLD?

HOW CAN WE APPROACH OTHERS TO EXPLORE WORKING TOGETHER?
(you could use an actual geographical map for this)

HOW CAN WE START TO DISCUSS INDIVIDUAL WORK AS PART OF A COLLECTIVE EFFORT?

COALITION MAPPING TEMPLATE

WHAT INFORMATION DO WE NOT HAVE?

WHO AND WHAT IS MISSING FROM THIS?

HOW CAN WE WORK TOGETHER TO SHARE AND BUILD?

WHAT RESOURCES DO WE NEED TO BUILD THE MOVEMENT?

WHO HAS ACCESS TO RESOURCE?

**WHAT KIND OF PEOPLE
OR GROUPS ARE ENGAGED
IN SIMILAR WORK?**

**WHERE IS THE WORK
TAKING PLACE?**

**WHAT SPECIALISM ARE NEEDED TO
BUILD A COLLECTIVE MOVEMENT?**

**WHAT VALUES AND PRINCIPLES
MUST GROUPS AND PEOPLE
BE ALIGNED WITH?**

**HOW CAN WE APPROACH OTHERS
TO EXPLORE WORKING TOGETHER?**

**HOW CAN WE START TO DISCUSS
INDIVIDUAL WORK AS PART
OF A COLLECTIVE EFFORT?**

**WHAT INFORMATION
DO WE NOT HAVE?**

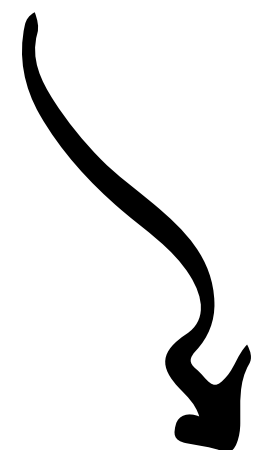
**WHAT SKILLS GAPS
DO WE HOLD?**

**HOW CAN WE WORK TOGETHER
TO SHARE AND BUILD?**

**WHAT RESOURCES DO WE NEED
TO BUILD THE MOVEMENT?**

**WHO HAS ACCESS
TO RESOURCE?**

**WHO AND WHAT IS
MISSING FROM THIS?**



PRINT ME!

COMMUNITY-CENTRED STRATEGIC LITIGATION

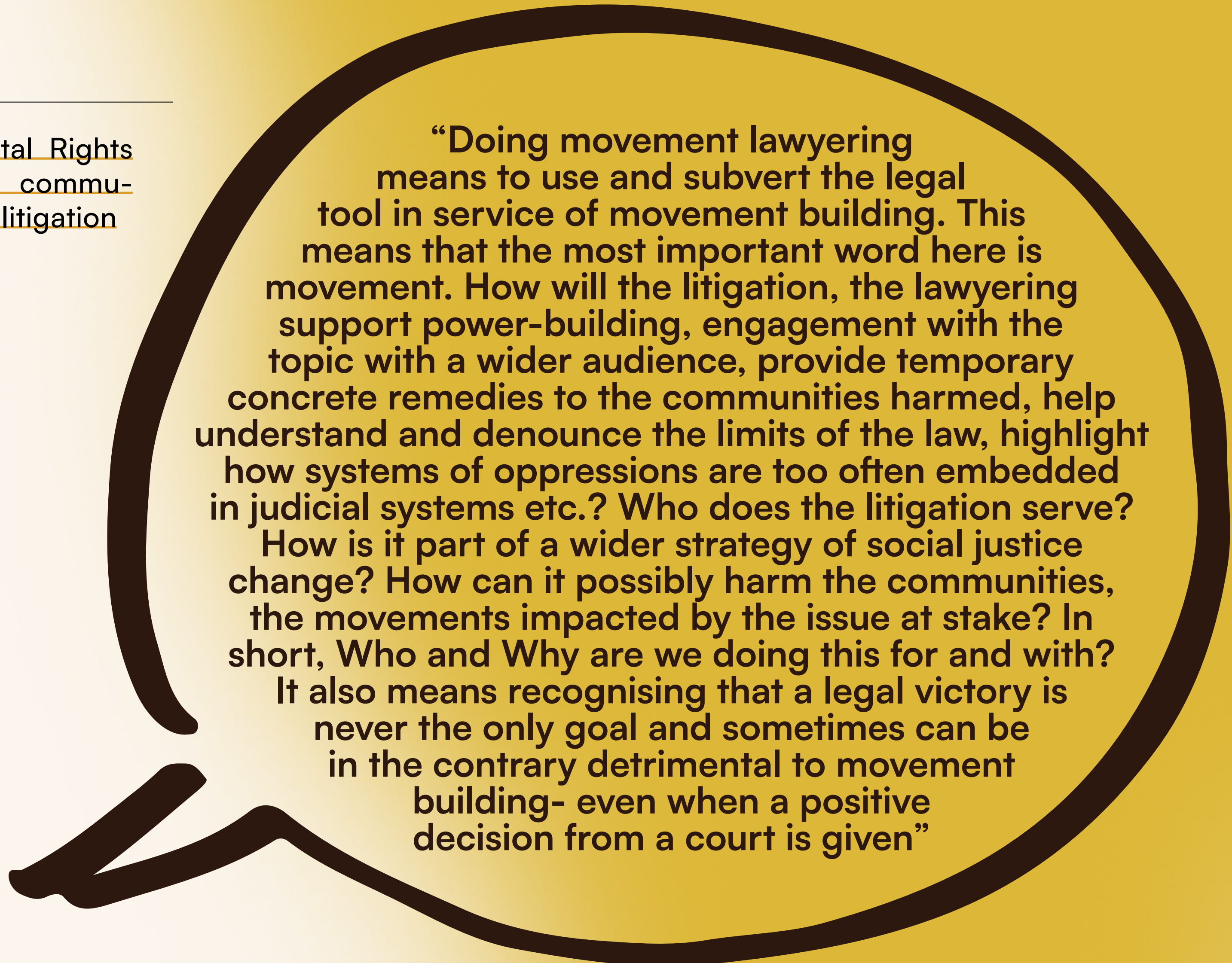
MOVEMENT LAWYERING

Laurence Meyer,
Co-director of **Weaving Liberation**

“Because it centres a community, community-centred strategic litigation aims at empowering its members and the organisations which defends its interests, it aims at building power within the community to enhance the capacity not only to react to and protect from current harms by the means they deem appropriate but also to imagine how to prevent those harms from reoccurring.

As is the case for strategic litigation in a more general sense, CCSL aims for collective change and not only for individual impact. Nonetheless, because it is led by the impacted community/communities at stake, the frontier between the individual and collective is not hermetic, those two notions – in the best-case scenario – are in dialogue. It uses the legal instrument as one of many methods of collective mobilisation in a wider strategy to bring about change.”

■ A season of Digital Rights for All: the case for community-centred strategic litigation



“Doing movement lawyering means to use and subvert the legal tool in service of movement building. This means that the most important word here is movement. How will the litigation, the lawyering support power-building, engagement with the topic with a wider audience, provide temporary concrete remedies to the communities harmed, help understand and denounce the limits of the law, highlight how systems of oppressions are too often embedded in judicial systems etc.? Who does the litigation serve? How is it part of a wider strategy of social justice change? How can it possibly harm the communities, the movements impacted by the issue at stake? In short, Who and Why are we doing this for and with? It also means recognising that a legal victory is never the only goal and sometimes can be in the contrary detrimental to movement building- even when a positive decision from a court is given”

CASE-STUDY THE MANCHESTER 10 IN THE UNITED KINGDOM

In 2022, ten young Black men were convicted, four for conspiracy to murder and six to conspiracy to cause grievous bodily harm. In their statement prior to the trial verdict the organisation Kids of Colour stated: ‘There has been no murder. There has been harm committed by a small minority, which has been admitted to. There is no victim at the centre of this case. While we do not seek to minimise the harm caused, as defence teams have argued, there was no intention or agreement to murder, and that has been denied by all. Two have pleaded guilty to the GBH count.’

All of the ten young Black men convicted had lost a friend who was murdered. The four convicted for conspiracy to murder were convicted based on

being part of a Telegram group, created following the death of their friend. As stated in a guardian article ‘none of the four had any weapons, nor took part in any violent acts or ‘scoping missions’ to locate individuals to be targeted for violence.’ They were condemned to 8 years in jail.

Kids of Colour followed the process and put in place actions to challenge the idea that this trial, using the problematic legal ground of joint enterprise, could bring any justice to the harm that was committed while also highlighting how the joint enterprise legal ground was used to criminalise young Black men just because of the music they listened to, the friends they had and their reactions to losing a friend on a Telegram chat few hours after learning about it.



In addition to organising de- 73
monstrations and sharing what
was happening in the court on social
media—hereby challenging the narra-
tive put in place to portray the group as
members of a gang – they organised a
community support campaign, asking
community members what they would
offer to these young men if the sentence
was suspended to ensure accountability
and mentoring, among other things.

‘In June 2022 we asked you to offer
your skills, expertise and care to 10 boys
facing prison sentences, to show that as a
city, we wanted suspended sentences, and
healing-centered approaches to youth
violence. Over 500 of you contributed,
and your commitments were incredible.’
They received 517 responses, from
individuals and organisations, ranging
from attending monthly accountability
meetings, regular phone calls, access to
networks to ensure employment, to loss
and grief support, childcare support, and
access to non-educational activities such
as music or sport. This community sup-
port showed concretely how different,
multifaceted answers to harm could be
put in place, outside of the prison system.
The report was shared during the trial by
the defendant lawyer to strengthen the
legal argument for suspended sentences.
It made abundantly clear how the judi-
cial system wasn’t fit to repair harm and
provide healing, while also making other
pathways to justice tangible in a collec-
tive imagining effort.

RESISTING DIGITAL POLICING TOOLKIT: BIBLIOGRAPHY

Abolitionist Futures
Reading List (2022).
<https://abolitionistfutures.com/reading-lists>

Amnesty International, (2020)
We sense trouble: Automated
discrimination and mass
surveillance in predictive
policing in the Netherlands.
[https://www.amnesty.org/en/
documents/eur35/2971/2020/en/](https://www.amnesty.org/en/documents/eur35/2971/2020/en/)

Bristol Gov. (2023, September).
Police and council defend
safeguarding app after calls
to stop collecting info on vulnerable
young people. Bristol Cable.
<https://thebristolcable.org/2023/09/>

[police-and-council-defend-safeguarding-app-after-calls-to-stop-collecting-info-on-vulnerable-young-people/](#)

BROWNE, S. (2015) *Dark Matters, On the Surveillance of Blackness*,
Duke University Press.

CANGIANO, A. (2010). Current
data on international migration
and migrants in the UK: implications
for the development of the Migration
Observatory at Oxford. ESRC Centre
on Migration Policy and society.
[http://migrationobservatory.
ox.ac.uk/wp-content/
uploads/2016/05/AlessioToR.pdf](http://migrationobservatory.ox.ac.uk/wp-content/uploads/2016/05/AlessioToR.pdf)

Census. (n.d.). 2023.
[https://www.census.gov/
programs-surveys/acs/
news/updates/2023.html](https://www.census.gov/programs-surveys/acs/news/updates/2023.html)

COLACICCHI, P. (2008). Profiling
and Discrimination against Roma
in Italy: New Developments in a
Deep-Rooted Tradition. *Roma
Rights Journal*, 2, 35—44.
[https://www.errc.org/
uploads/upload_en/file/03/
B8/m000003B8.pdf](https://www.errc.org/uploads/upload_en/file/03/B8/m000003B8.pdf)

CRESTO-DINA, L. (2023, May 31).
Police Technology and its dangers
— The Gangs Matrix as a case study
of potential data-driven harms.
Sanders Law News.
<https://www.saunders.co.uk/>

[news/police-technology-and-its-dangers-the-gangs-matrix-as-a-case-study-of-potential-data-driven-harms/](#)

DAY, A. S., & McBean, S. O.
(2022). *Abolition revolution*.
Pluto Press; Pluto Press Inc.

Data Justice Lab. (2022) Top400,
a Top-down crime-prevention
strategy in Amsterdam.
[https://datajusticelab.
org/2022/12/08/new-research-
report-top400-a-top-down-crime-
prevention-strategy-in-amsterdam/](https://datajusticelab.org/2022/12/08/new-research-report-top400-a-top-down-crime-prevention-strategy-in-amsterdam/)

Digital Freedom Fund. (2021). Extraction of asylum seeker mobile data in Germany. Digital Freedom Fund. <https://digitalfreedomfund.org/extraction-of-asylum-seeker-mobile-data-in-germany/>

Digital Freedom Fund. (2023). “Talking Digital Lexicon” <https://digitalfreedomfund.org/digital-rights-for-all-talking-digital-toolkit/>

Euromed Rights. (2023). “Artificial intelligence: The new frontier of the eu’s border externalisation strategy (pp. 18—19). Euromed Rights” https://euromedrights.org/wp-content/uploads/2023/07/Euromed_AI-Migration-Report_EN-1.pdf

European Data Protection Board. (2021) “Swedish DPA: Police unlawfully used facial recognition app” https://www.edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en

EDRi, “Greek Ministry of Asylum and Migration face a record-breaking €175,000 fine for the border management systems

KENTAUROS & HYPERION”, (2024). <https://edri.org/our-work/greek-ministry-of-asylum-and-migration-face-a-record-breaking-e175000-fine-for-the-border-management-systems-kentauros-hyperion/>

EDRi, (2024) “SHARE Foundation presents #hiljadekamera: A documentary on biometric mass surveillance” <https://edri.org/our-work/share-foundation-presents-hiljadekamera-a-documentary-on-biometric-mass-surveillance/>

HALL, S. (1978). “Policing the crisis: Mugging, the state, and law and order”. Holmes & Meier.

HAMID, S. T. (2020). “Community Defense: Abolishing Carceral Technologies”. Logic(s), Care (11). <https://logicmag.io/care/community-defense-sarah-t-hamid-on-abolishing-carceral-technologies/>

Homo Digitalis, (2022) “The Hellenic DPA is requested to take action against the deployment of ICT systems IPERION & KENTAUROS in facilities hosting asylum seekers in Greece” <https://homodigitalis.gr/en/posts/10874/>

KIMBELL, J. (2023, October). “The growth of digital policing: Enhancing efficiency and safety through technology”. GovNet. <https://blog.govnet.co.uk/justice/the-growth-of-digital-policing>

Lighthouse Reports. “Suspicion Machine” (2023). <https://www.lighthousereports.com/investigation/suspicion-machines/>

LOTHIAN-MCLEAN, M. (2022, July 30). “Racism row as Manchester police ban people ‘linked to gangs’ from carnival”. The Guardian. https://www.theguardian.com/uk-news/2022/jul/30/manchester-police-under-fire-over-deeply-racist-tactics-ahead-of-caribbean-carnival?CMP=share_btn_url

MCDOWELL, M. G., & Fernandez, L. A. (2018). “Disband, disempower, and disarm: Amplifying the theory and practice of police abolition”. Critical Criminology, 26(3), 373—391. <https://doi.org/10.1007/s10612-018-9400-4>

MCQUILLAN, D. (2022). “Deep Learning and Human Disposability: AI is a technology for managing social murder”. Logic(s), 17.

<https://logicmag.io/home/deep-learning-and-human-disposability/>

MUHAMMAD, K. G. (2010) “The condemnation of Blackness, Race, Crime and the making of Modern urban America” Harvard University Press
MUÑIZ, A. (2015). “Police, power, and the production of racial boundaries” Rutgers University Press.

Nteboheng Maya Mokuena, (2024) “Playing Games with Rights: A Case Against AI Surveillance at the 2024 Paris Olympics”, Georgetown Law Technology Review. <https://georgetownlawtechreview.org/playing-games-with-rights-a-case-against-ai-surveillance-at-the-2024-paris-olympics/GLTR-05-2024/>

Oracle. (2023). “What Is a Database?” <https://www.oracle.com/database/what-is-database/>

OZKAN, E., & STEVENS, S. (2021, February 18). “Policing in Europe: The Nexus Between Structural Racism and Surveillance

Economies”. The London School of Economics and Political Science.
<https://blogs.lse.ac.uk/mediase/2021/02/18/policing-in-europe-the-nexus-between-structural-racism-and-surveillance-economies/>

Statewatch (2022). “Building the biometric state: Police powers and discrimination”
<https://www.statewatch.org/publications/reports-and-books/building-the-biometric-state-police-powers-and-discrimination/>

Statewatch (2022). “Europol management board in breach of new rules as soon as they came into force”
<https://www.statewatch.org/news/2022/november/europol-management-board-in-breach-of-new-rules-as-soon-as-they-came-into-force/>

Strasbourg (2022, June 29). “Council of Europe launched a new network of national law enforcement correspondents. Council of Europe News”
<https://www.coe.int/en/web/human-rights-rule-of-law/-/creation-of-a-network-of-national-correspondents-of-police-authorities>

TechTarget (2023) “Data sampling”
<https://www.techtarget.com/searchbusinessanalytics/definition/data-sampling>

Thales. (2023, September 8). “Biometrics in law enforcement. Digital Identity & Security Blog”.
<https://dis-blog.thalesgroup.com/identity-biometric-solutions/2023/09/08/biometrics-in-law-enforcement/>

Weeks, T. (2022, May). “The digital policing promise”
Digital Leaders.
<https://digileaders.com/the-digital-policing-promise/>

SOME OTHER USEFUL RESOURCES

76

Surveillance Watch is an interactive map revealing the intricate connections between surveillance companies, their funding sources and affiliations. On the website you can find which companies is selling which type of digital policing tools to which country.
<https://www.surveillancewatch.io/>

Ctrn is a space of convening for those organizing against the design, experimentation, and deployment of carceral technologies.
<https://www.carceral.tech/>

No Tech for Tyrants. (2022) “Surveillance Tech Perpetuates Police Abuse of Power”
https://notechfortyrants.org/wp-content/uploads/2022/11/NT4T_Report_FINAL_web.pdf

Street level surveillance hub from EFF: <https://sls.eff.org/>

Stop LAPD spying report and resources: <https://stoplapdspying.org/reports-resources/>

Just Futures Law resources:
<https://www.justfutureslaw.org/resources>