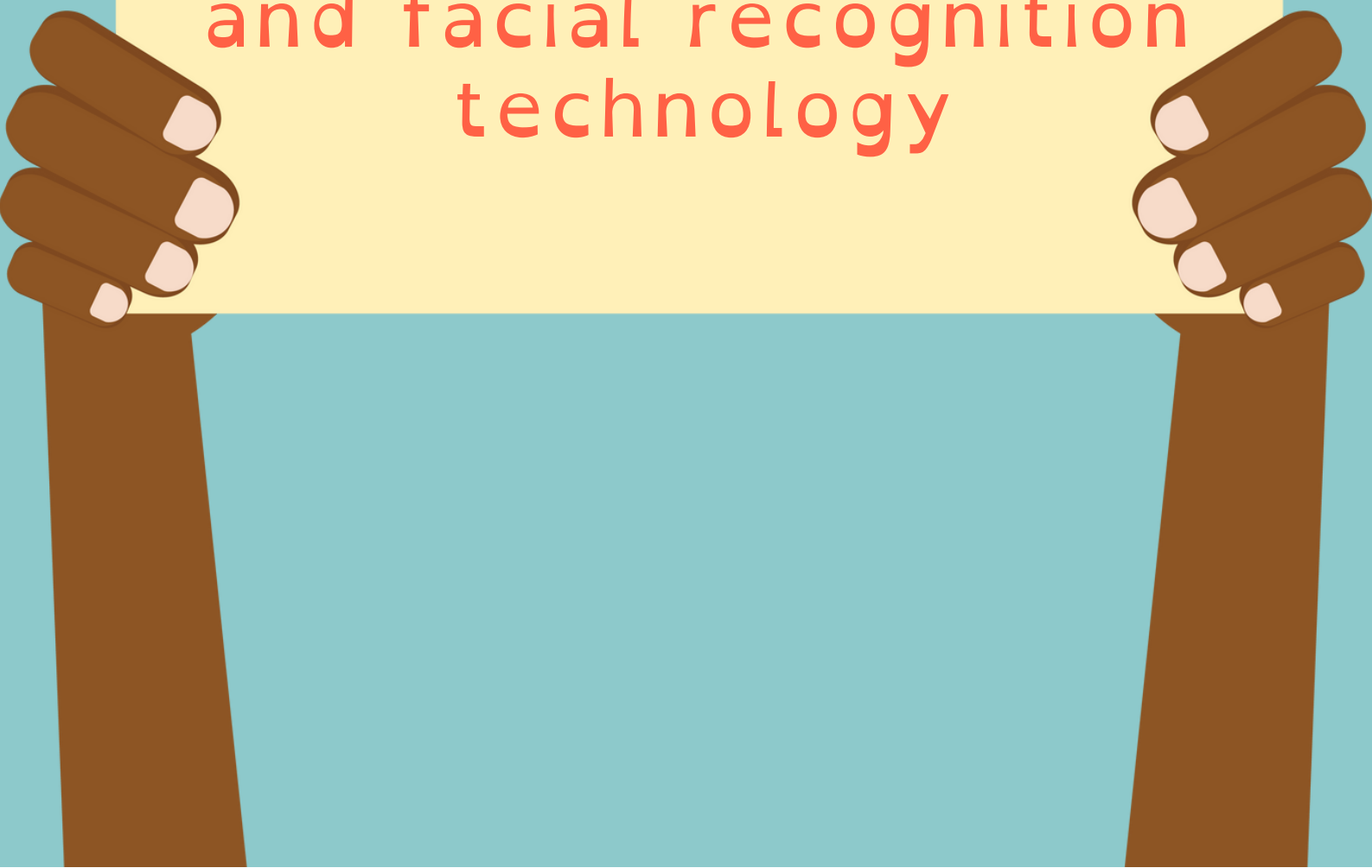
THE RACIAL JUSTICE NETWORK

YORKSHIRE RESISTS
THE HOSTILE ENVIRONMENT

#HandsOffOurBiodata:

Mobilising against police use of biometric fingerprint and facial recognition technology



CONTENTS

ABOUT US

The Racial Justice Network (RJN) is an anti-racist charity based in West Yorkshire. RJN brings together groups, organisations and individuals from across the West Yorkshire region (and beyond) to proactively promote racial justice and address colonial legacies.

Our organisation aims to raise awareness about, and mobilise around, racial inequality and injustice by listening and working with disempowered communities, taking positive action for justice and solidarity.

Yorkshire Resists is a network of organisations and individuals working to resist the Hostile Environment across Yorkshire. Together with RJN we launched the #StopTheSCANdal campaign to fight against the implementation of biometric fingerprint scanners across West Yorkshire.

To cite this report:
Loyola-Hernández, L., Coleman, C., Wangari-Jones, P. and Carey, J. (2022) *#HandsOffOurBiodata: Mobilising against police use of biometric fingerprint and facial recognition technology*, the Racial Justice Network and Yorkshire Resists, UK.

We would like to thank Big Brother Watch for their support in obtaining the Freedom of Information requests on our behalf.

Dyslexic-friendly design and font (open dyslexic size 13, 1.5 line spacing, 12 letter spacing)

FORWARD BIG BROTHER WATCH

From live facial recognition to mobile fingerprint scanners, the accelerating rollout of biometric technology by police forces poses a serious threat to privacy and civil liberties and may exacerbate the worrying racial disparities we already see in policing.

This report has uncovered important evidence that People of Colour are much more likely to be stopped and subjected to a fingerprint scan on the street than white people. The report is a critical exposé of a new aspect of technology-facilitated discriminatory policing and a call to action for the regulation, oversight and institutional change necessary to right this wrong.

Suspicionless surveillance powers have no place in a healthy democracy at all, eroding privacy for everyone and seeding injustice particularly for racialised and marginalised people. Years of stop and search data show that Black men are significantly overrepresented, and disproportionately treated with suspicion by police. The introduction of mobile fingerprint scanners to be used at an officer's discretion for several reasons, including subjective doubt about the name someone has given to police, appears to be continuing and exacerbating racial disparity in police use of suspicionless surveillance powers.

Mobile fingerprint scanners are allowing police forces to moonlight as border control with several forces running prints against the Home Office immigration database, as well as police records, by default. In a society where ethnic minorities are consistently over-policed this is one step further on the road to a “papers please” Britain.

The UK Government does not universally require people to carry identification. Big Brother Watch has been at the forefront of the battle against the state’s efforts to require people to carry identification documents just to exist. Street deployments of biometrics, including mobile fingerprint scanners and facial recognition, undermine an individual’s right to walk down the street anonymously and exacerbate a two-tier society. Wide discretion is given to police officers who "doubt" the details someone has given them to use biometric scanning with minimal oversight.

Individuals do not need to be licensed to exist by the state – rather, the state exists on the licence of the people. Yet mobile biometrics are threatening to lead us down the road to compulsory ID by the back door. This report provides vital and timely evidence of the injustice of biometric Britain, and is a compelling call for change.

Jake Hurfurt
Head of Research and Investigations
Big Brother Watch

CONTEXT 2020-2022

Over the past two years, we have all experienced - often in very different ways – the accumulation of global and local challenges. Many of these "challenges" are steeped in histories of racism, colonialism, and class struggle. All inflict new wounds. How do we begin to describe what has taken place?

We have suffered the devastation brought by a global pandemic. We know the isolation of lockdowns and the exposure to the COVID-19 virus was not evenly borne. **We have protested and grieved the continued state-sanctioned violence against Black and Brown people in police custody in the UK.** Many have experienced another kind of grief when, yet again, this attention is determined by the length of a news cycle. On 5th September, 2022 Chris Kaba, 24, was murdered by the London Metropolitan Police. Today his name is absent from the BBC News homepage.

We have witnessed a sustained attack on civil liberties and human rights. The Police, Crime, Sentencing and Courts Act has eroded rights to protest enshrined in the Human Rights Act. **The Nationality and Borders Act introduces a raft of measures that create obstacles and harms to people seeking asylum: increasing arbitrary procedural demands that push people into undocumented status; creating routes of unsafety; and exacerbating precarity.** The Rwanda deal, which seeks to process asylum claims and offshore people seeking asylum to Rwanda, has violated the principle of the UN Refugee Convention to grant fair [illegible] on U[illegible]il.

The Conservative government has pushed through plans condemned across society as inhumane. In doing so, this government has laid bare its commitment to forsaking the tenants of sanctuary and justice. Now we face the Cost of Living crisis and a Prime Minister unwilling to take the measures necessary to sufficiently support those hit hardest.

Yet, at a time dominated by narratives of "a world standing still", we saw the momentum of Direct Action. The Black Lives Matter movement urged the UK to come to terms with its own history and reality of police brutality. The toppling of the Edward Colston statue in Bristol and the success of anti-raids networks at Kenmure Street, Glasgow and Lewisham, London, reminded us that **Direct Action is not only necessary, but possible.**

Throughout all this, oppressed and marginalised communities, and those who seek to stand alongside them, have sought to respond to the challenges faced; from Black Lives Matter and the Kill the Bill protests to the nation-wide Union strikes and vital acts of community care. **At the Racial Justice Network and Yorkshire Resists, we seek to stand alongside those who mobilise against oppression and marginalisation. This report marks another step in that direction.**

This report is part of the Racial Justice Network and Yorkshire Resists campaign, #StopTheSCANdal, to draw attention to the impact of the Biometric Services Gateway and the new pilot Operator Initiated Facial Recognition (OIFR) app on both the communities targeted by police for fingerprinting and facial scanning as well as the wider public.

There has been no public consultation on the roll out of the devices, nor consideration of the harmful aspects of the fingerprint scanner, OIFR app and sharing of biometric data. **We are concerned and alarmed about the disproportionate use of BSG and facial recognition software on racially minoritised and migrant communities.** You can find more information about the Stop The Scan campaign and how the Biometric Services Gateway works here: www.stopthescan.co.uk

SUMMARY

- 24 police forces, that we know of, are currently using the Biometric Service Gateway app (fingerprint mobile app).

- South Wales Police are the only force in the UK piloting the facial recognition mobile app (Operation Initiated Facial Recognition). It is extremely worrisome this technology has been rolled out after South Wales Police lost a court case on facial recognition brought by Liberty. The court determined the police had 'breached privacy rights and broke equalities law' (see Liberty 2022).

- 11 police forces refused to respond to our FOI under Section 12(1) 'excess time and resources'. Only 7 provided clear data on arrests, 8 on ethnicity, 2 on gender, 5 on reason for scan and 0 on the location of the stop and scan.

- The Section 12(1) justification, and the lack of justification for the omission of key data points, is unacceptable in the context of increased public awareness of police misuse of powers and public interest in the monitoring of issues around ethics, discrimination and racial profiling.

- The data that was provided shows a clear bias in who is targeted by stop and scan practices. It is therefore alarming that a number of other forces either did not collect, or refused to provide, these statistics.

- Black people are 4 times more likely to be stopped and scanned than a white person. Asian people are 2 times more likely to be stopped and scanned than a white person.

- Men are 12 times more likely to be stopped and scanned than those identified as 'Women' or 'Unknown' by officers. Police do not input information regarding trans people, non-binary or gender non-conforming people. Facial recognition follows a similar trend.

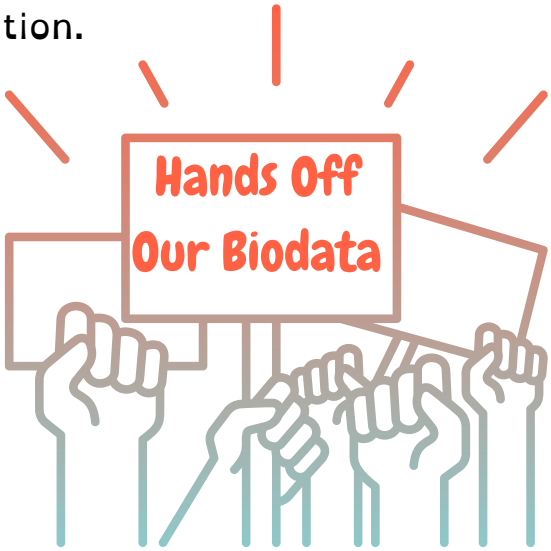
- A high number of police forces are using biometric fingerprint technology for immigration enforcement.

- 6 forces are scanning the immigration and criminal databases simultaneously. This marks a departure from earlier approaches and no justification was provided for this shift. Crucially, it exacerbates the damaging conflation of immigration with criminal activity.

- The facial recognition mobile app was used 42 times in the ongoing pilot stage, on 35 people. Of these individuals, six were minors between the ages of 10-17.

- Mobile fingerprinting and facial recognition is pursued to cut police time and costs (see for example: BBC London 2019). The pursuit of 'efficient policing' undermines responsibilities to protect communities.

- This is reflected in the reasons provided for a stop and scan. Most scans were conducted because the officer doubted the person's details were real or suspected the person had committed a crime. In other words, it circumvents the need to provide sufficient grounds for arrest and to take individuals to the police station.



BIOMETRIC FINGERPRINT TECHNOLOGY

The Biometric Service Gateway (BSG) retrieves data from particular databases, interprets it, performs the necessary actions and sends it back to the mobile device. This system allows personal information to be quickly requested and shared between law enforcement and immigration enforcement. Practically speaking, the technology consists of an app on a police officer's phone, along with a mobile fingerprint scanner. It can be used to almost instantly check fingerprints against those stored on either the Immigration and Asylum Biometric Database (IABS) or IDENT1 (law enforcement database).

The scanners can be connected to any mobile phone or tablet running the corresponding app that enables the biometric databases to be searched. Their use is regulated under Section 61(6A) of the Police and Criminal Evidence Act 1984 (PACE)25 and further outlined in the PACE Code D (2017)26. Section 61 PACE and Code D also provide officers with the power to take a fingerprint by force by virtue of Section 117 of the Act.

The Biometric Services Gateway (BSG) is a portal that connects an app on a phone or mobile device to two databases. First, the Home Office (through the Immigration and Asylum Biometrics System (IABS) database) and second, the police (through the IDENT1 database used by law enforcement agencies).

The use of the scanners differs from Stop and Search in that officers can only scan the fingerprints of an individual in the case that:

- An offence has been committed (or suspected to have been committed).
- Either no name is provided by the individual OR the name provided is suspected to be false.

Anyone suspected of committing a crime or 'lying' about their identity can be stopped in the street and have their fingerprint scanned on the spot and searched in the police and immigration databases (RJN 2021: 10). Officers use their own discretion to determine how authentic or reliable a given identity is. Accordingly, this is a subjective judgement that has the potential to lead to even further discrimination against, for example, trans or non-binary people within Black and Brown communities.

Anyone with a migrant status (e.g., someone on a visa, with Indefinite Leave to Remain, asylum seekers, refugees or precarious migrant status) will have their fingerprint in the Home Office immigration database (IABS). They will trigger an alarm on the app if scanned by the police. The police are obliged to contact the Home Office (e.g., phoning Command and Control units) to clarify if there is a need to detain a person due to an immigration issue.

STOP AND SCAN PROCESS

1. Officers discretion as to what constitutes an offence.
2. Officer judges whether the person is who they say they are.
3. Officer can search criminal, immigration or both data bases.
4. Flag is returned if there's activity linked to person (i.e. on a visa).
5. If flag returned officer must call Home Office Command and Control.
6. Home Office might put person in indefinite detention or deport them.

KEY FINDINGS FINGERPRINT APP

This report details data collected via Freedom of Information (FOI) requests concerning police use of mobile fingerprinting scans using BSG. We sent an FOI request to all police forces in the UK (England, Wales and Scotland) except two special police forces (Civil Nuclear Constabulary and Ministry of Defence). This resulted in requests to forty-four territorial police forces and one special police force (British Transport Police). The request asked for police statistics for the period between April 2020 and December 2021.

11 out of 46 police forces refused our FOI under section 12(1) excess of time and resources:

- Bedfordshire
- Cambridgeshire
- City of London
- Derbyshire
- Devon and Cornwall
- Dorset
- Durham
- Hertfordshire
- Met Police
- North Yorkshire
- Nottinghamshire

In comparison with our previous FOI request in 2020, there was a small decrease (6) in police forces refusing. Those that have consistently refused both FOIs are:

- Bedfordshire
- Cambridgeshire
- Durham
- Hertfordshire
- Nottinghamshire

Based on our FOIs, currently **13 police forces do not use the Biometric Gateway Service.** These are:

- British Transport Police
- Cleveland
- Cumbria
- Greater Manchester
- Gwent
- Humberside
- North Wales
- Police Scotland
- South Wales
- South Yorkshire
- Staffordshire
- Warwickshire
- West Mercia

Northumbria replied saying they did not have this information, neither confirming or denying they use (or don't) the BSG.

Of those police forces not using the Biometric Gateway Service, **5 have plans to use them in future.** These are:

- British Transport Police (July-August 2022)
- Greater Manchester (no date confirmed)
- North Wales (considering nothing confirmed yet)
- South Yorkshire (no date confirmed)
- Staffordshire (May-September 2022)

Of police forces who were not using the BSG at the time of our last FOI request in 2020, but stated they had plans to, 3 have since started using biometrics:

- Avon and Somerset
- Hampshire
- Thames Valley

There has been an increase of 9 police forces using BSG since our last FOI in 2020. Twenty four forces who responded to our most recent FOI (2022) use the Biometric Gateway Service. These are:

- Avon and Somerset
- Chesire
- Dyfed-Powys
- Essex
- Gloucestershire
- Hampshire
- Kent
- Lancashire
- Leicestershire
- Lincolnshire
- Merseyside
- Norfolk
- Northern Ireland
- North Yorkshire
- Northamptonshire
- Staffordshire
- Suffolk
- Surrey
- Sussex
- Thames Valley
- West Midlands
- West Yorkshire
- Wiltshire
- Met Police (refused our FOI, but their use is confirmed elsewhere).

24 police forces use the biometric fingerprint app

Gwent police once used the BSG in joint operation with the Met in April 2021.

There has been an increase in the number of devices equipped with the capacity to search the BSG. We have the following data from FOIs:

- West Midlands police started to purchase devices in 2018-19 with a total of 121 and in 2019/2020 purchased 450 more.
- Dyfed-Powys police currently own 35 mobile fingerprint scanners.

We have the following information from supplementary research (see Stop the Scan 2020 and BBC London 2019):

- West Yorkshire Police started with 9 devices in 2018. This increased to 250 in 2019.
- Met Police had developed 550 of their own mobile devices (to access the BSG).
- 2019 saw a growth of 3000 to 9000 "users" (e.g., officers and sergeants) from the Met Police using the device.
- Met Police stated they had plans to put out 220 more devices by the end of 2019. This would take their total to 770 devices.

This means there were approximately **at least** 1626 devices in use by the end 2020. The real number is expected to be far higher given more forces were using the device and that numbers may have increased by 2022.

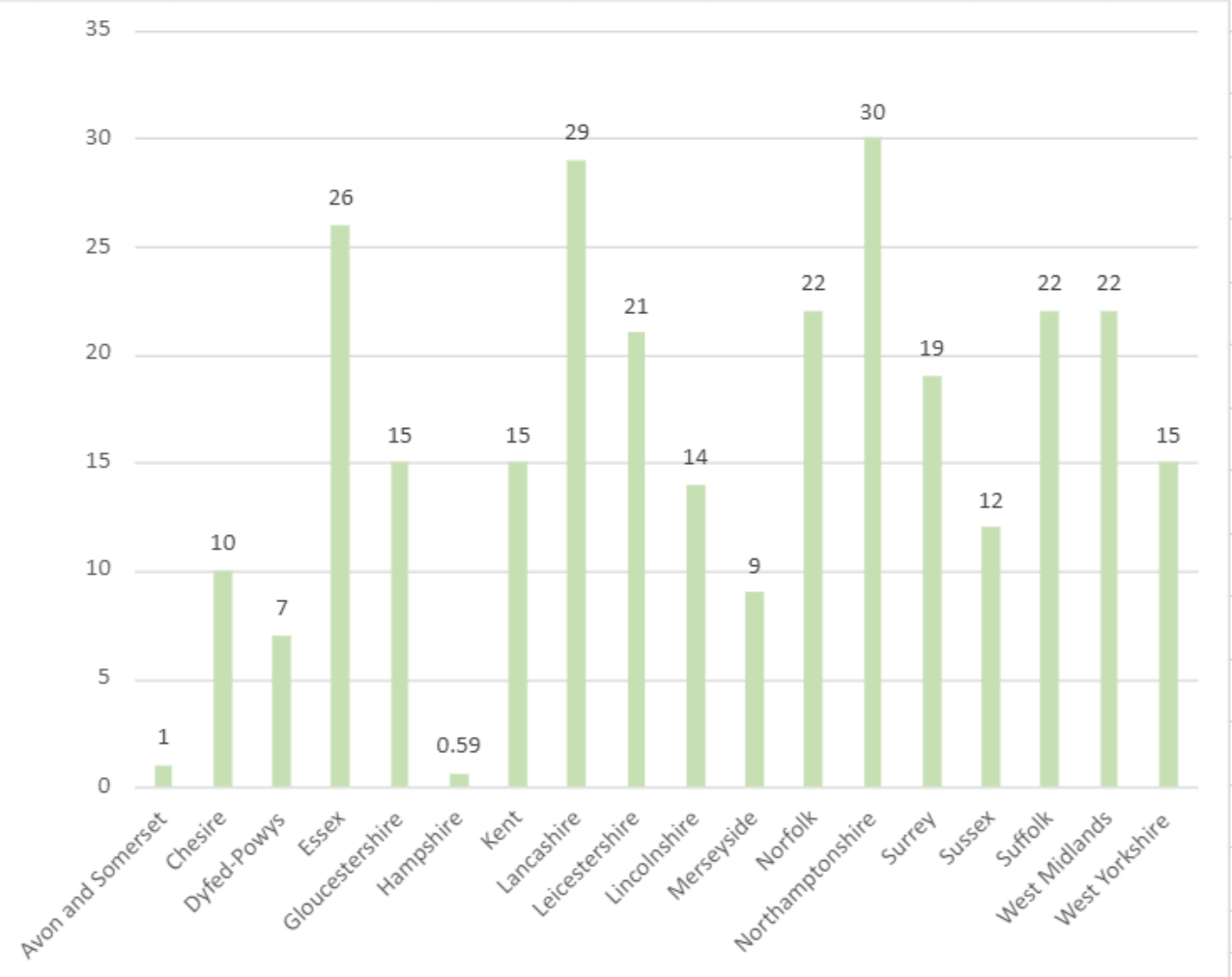
The West Yorkshire Police and the Metropolitan Police have directly heard the criticisms levied at them by non-governmental organizations and impacted individual and communities. They are also aware that these actors have raised questions around ethical procedures and reviews of the devices. These questions remain unanswered.

It is therefore with concern and frustration that we note the rate at which significant numbers of these devices have been introduced.

At least 1626 (est.) devices in use by 2020

9000 Met Police users in 2019

NUMBER OF SCANS PER 10,000 RESIDENTS



The highest number of scans per area are Northamptonshire Police (30 in 10,000), Lancashire Police (29 in 10,000) Essex Police (26 in every 10,000), Norfolk and Suffolk Police combined (information presented like this in FOI response) (22 in 10,000) and West Midlands Police (22 in 10,000).

6,446 scans

West Midlands police carried out the largest amount of scans (of forces that provided information).

Of the forces who provided further information on the number of scans and the database searched, the total number of scans from April 2020 to December 2021 per force are:

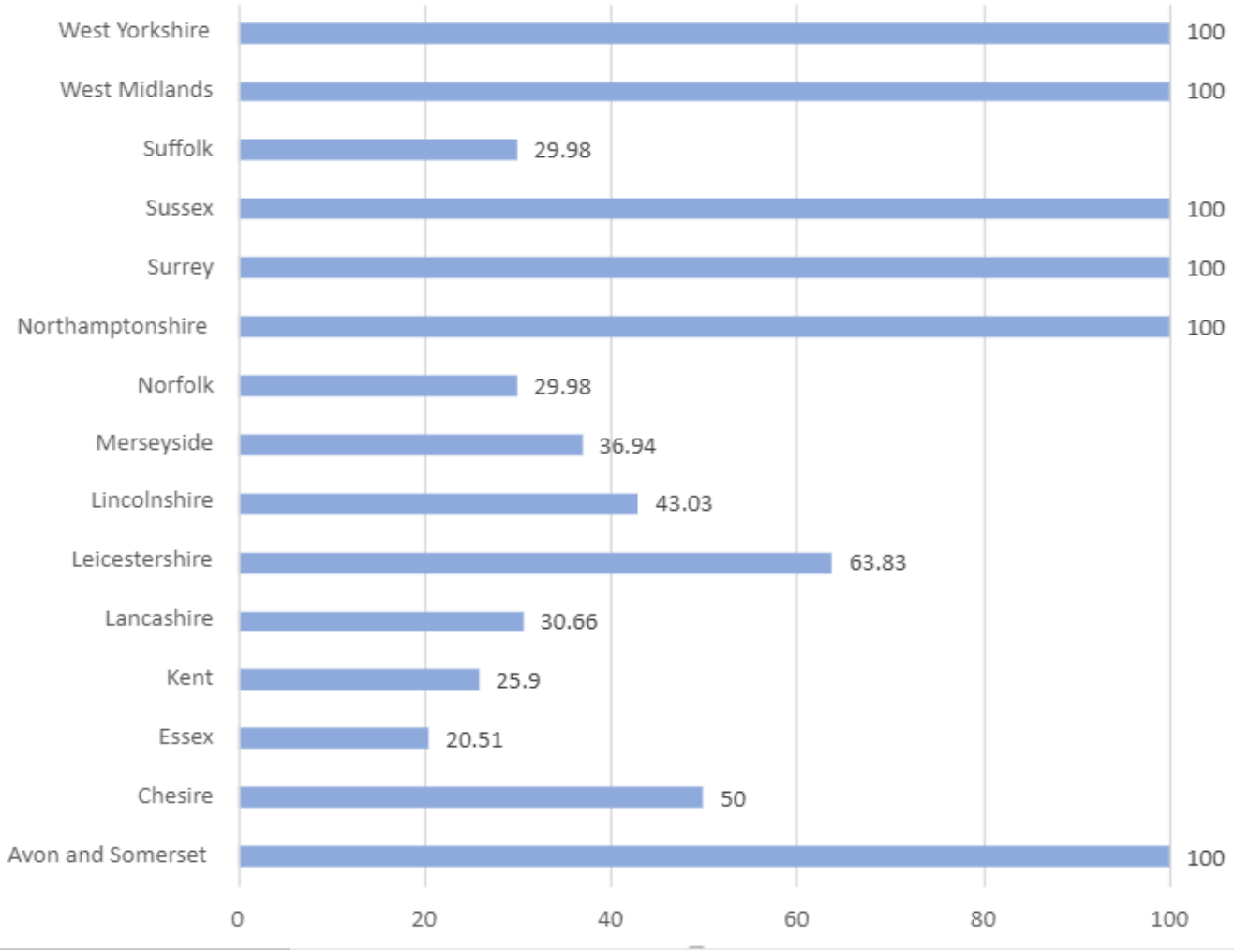
Police force	IABS (immigration)	IDENT1 (police)	Both	Total
Avon and Somerset	N/A	N/A	42	204 (since Dec 2021) *only had info on 42 of searches
Chesire	479	479	N/A	958
Dyfed-Powys	no info provided	no info provided	N/A	341
Essex	954	3,697	N/A	4,651
Gloucestershire	no info provided	no info provided	N/A	940
Hampshire	no info provided	no info provided	N/A	119
Kent	691	1,976	N/A	2,667
Lancashire	30	2,950	1,275	4,255
Leicestershire	56	738	1,275	2,085
Lincolnshire	19	574	420	1,020

There is no consistent approach regarding whether fingerprints are checked against the IABS and IDENT1 databases separately or simultaneously. The below figures suggest approaches differ substantially. No police force disclosed a justification, explanation or rationale for their approach.

Police force	IABS (immigration)	IDENT1 (police)	Both	Total
Merseyside	494	843	N/A	1,337
Norfolk (with Suffolk)	647	1,511	N/A	2,158
Northamptonshire	N/A	N/A	2,039	2,039
Surrey	N/A	N/A	2,039	2,039
Sussex	N/A	N/A	2,055	2,055
Suffolk (with Norfolk)	647	1,511	N/A	2,158
West Midlands	N/A	N/A	6,446	6,446
West Yorkshire	N/A	N/A	3,298	3,298

Of those police forces that did provide disaggregated data between checks on the immigration database and the police database, six stated that they routinely conduct checks on both databases simultaneously. This marks a departure from our previous understanding, particularly from previous statements made by West Yorkshire Police, that all searches of databases are conducted separately.

PERCENTAGE OF IMMIGRATION SCANS OUT OF TOTAL SCANS



In addition to the results detailed in the table above, **Avon and Somerset, Northamptonshire, Surrey, Sussex, West Midlands and West Yorkshire Police checked both immigration and police databases automatically.** This both reflects and entrenches the damaging conflation of immigration with criminal activity. In addition, Cheshire, Essex, Kent, Merseyside, Suffolk and Norfolk police forces carried out a high number of checks specifically because of an immigration reason. In short, this technology is increasing the pervasive trend towards the criminalisation of migration.

This indicates that the **police have fully taken on board immigration and border guard duties. Potential immigration status alone can be a justification for police intervention and law enforcement.** This puts migrants already traumatised and marginalised by Hostile Environment policies in an even more vulnerable position. This is particularly evident when migrant survivors of abuse and hate crimes are deterred from seeking help from the police out of fear of having their data shared with Immigration Enforcement. On this issue see, for example, Liberty and Southhall Black Sisters' super-complaint on data-sharing between the police and Home Office regarding victims and witnesses to crime, as well as the Step Up Migrant Women campaign led by LAWRS.

Scans that led to matches and/or arrests

Immigration

Focusing on immigration scans, **West Midlands Police overwhelmingly have the highest proportion of search "success" where the Home Office Biometrics (HOB) gateway has provided a response** (but not necessarily a match). It was unclear if it led to arrest in the case of West Midlands Police.

Police force	Total immigration scans (IABS only and IABS + INDENT 1)	No. of matches and/or arrests from immigration scans	% arrests and/or matches from scans
Avon and Somerset	42	1	2.38%
Cheshire	479	61	12.73%
Essex	954	212	22.22%
Norfolk and Suffolk	647	171	26.42%
Northamptonshire	2,039	25	1.22%
West Midlands	6,446	3,721	57.72%

Scans that led to matches and/or arrests

Police

Focusing on police scans using the criminal database IDENT1, again **West Midlands Police overwhelmingly have the highest proportion of search** success where the Home Office Biometrics (HOB) gateway has provided a response (but not necessarily a match). It was unclear if it led to arrest in the case of West Midlands Police.

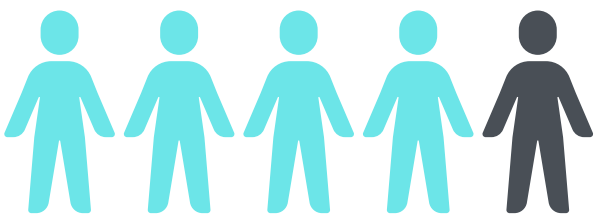
Police force	Total police scans (INDENT 1 only or + IABS)	No. of matches and/or arrests from police scans	% matches and/or arrests from scans
Avon and Somerset	42	20	47.61%
Cheshire	479	96	20.04%
Essex	3,697	1,354	36.62%
Norfolk and Suffolk	1,511	529	35%
Northamptonshire	2,039	241	11.81%
West Midlands	6,446	3,721	57.72%

Scans according to people's ethnicity

While in absolute numbers white North Europeans have been scanned the most, when compared to the percentage of resident population by ethnicity, **White Europeans consistently have the lowest rate of being stopped and scanned** according to the numbers of police forces who included this information in our FOI request. It is important to note that police did not provide disaggregated data of white population, instead only using the categories 'White North European' and 'White South European'. It is paramount we recognise the Gypsy, Roma and Traveller communities have continuously been criminalised by police, and that this will only get worse with the passing of the Police, Crime, Sentencing and Courts Act. Therefore, while statistics were not provided for these communities, it is extremely likely they are disproportionately impacted by stop and scan.

Percentage of scans according to ethnicity (calculated by the total number of scans)*

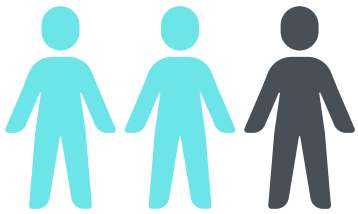
- White people represent 65% of total scans yet they represent 87.17% of total UK population.
- Black people represent 11% of total scans yet they represent 3% of the total UK population.
- Asian people represent 14% of total scans yet they represent 6.9% of total of UK population.
- Other ethnic minority people represent 5% of total scans yet they represent 0.9% of total of UK population.
- 5% of scans did not identify the ethnicity of the person being scanned.



Black people are 4 times more likely to be stopped and scanned than a white person

*using 2011 ethnicity data from Office for National Statistics.

Asian people are 2 times more likely to be stopped and scanned then a white person



These stark figures reveal the extent of racial bias embedded in the use of this technology. This data highlights the urgency to stop using this technology. It is disproportionately being used on racially minoritised communities. Causing individual and community trauma. The use of this technology does not keep our communities safe.

Stop and Scan According to Ethnicity

Police force	White North European	White South European	Black	North African	Asian	South East Asian	Arab/ Middle Eastern	Chinese/ Japanese	Dark European	Unkno-wn	TOTAL
Avon and Somerset	24	8	4	n/a	1	n/a	n/a	n/a	n/a	5	42
Chesire	618	52	88	4	108	12	28	22	n/a	26	958
Leicestershire	813	345	220	n/a	357	n/a	75	19	n/a	239	2068
Lincolnshire	718	76	60	n/a	60	n/a	34	3	n/a	69	1020
Northamptonshire	1058	339	285	n/a	156	n/a	39	21	n/a	5	1903
Surrey	1187	n/a	286	n/a	198	n/a	92	30	150	112	2055
Sussex	1235	n/a	253	n/a	150	n/a	92	15	169	135	2049
West Yorkshire	1689	263	272	n/a	822	n/a	82	61	n/a	108	3297
TOTAL	7342	1083	1468	4	1852	12	442	171	319	699	13,392

It is alarming given the long history of well-documented racial profiling and racial bias in police stop and search that most police forces are not collecting ethnicity information or did not provide it in order to monitor their execution of these scans.

West Yorkshire Police presented information with regards to ethnicity and reason of the person being arrested. Information is as follows:

Ethnicity	Offence (sec 61 PACE 1984)	Duty of care (mental capacity act 2005)	Deceased (coroners and justice act 2009)	Total
White Northern European	1068	184	437	1689
White Southern European	249	10	4	263
Black	211	32	29	272
Asian	764	34	24	822
Chinese/ Japanese	57	4	0	61
Middle Eastern/ Arab	77	1	4	82
Unkown	62	15	31	108
Total	2488	280	529	3297

Only two police forces provided the gender of the person being stopped and scanned:

- Avon and Somerset scanned 9 women and 33 men
- Surrey scanned 145 women versus 1,904 men

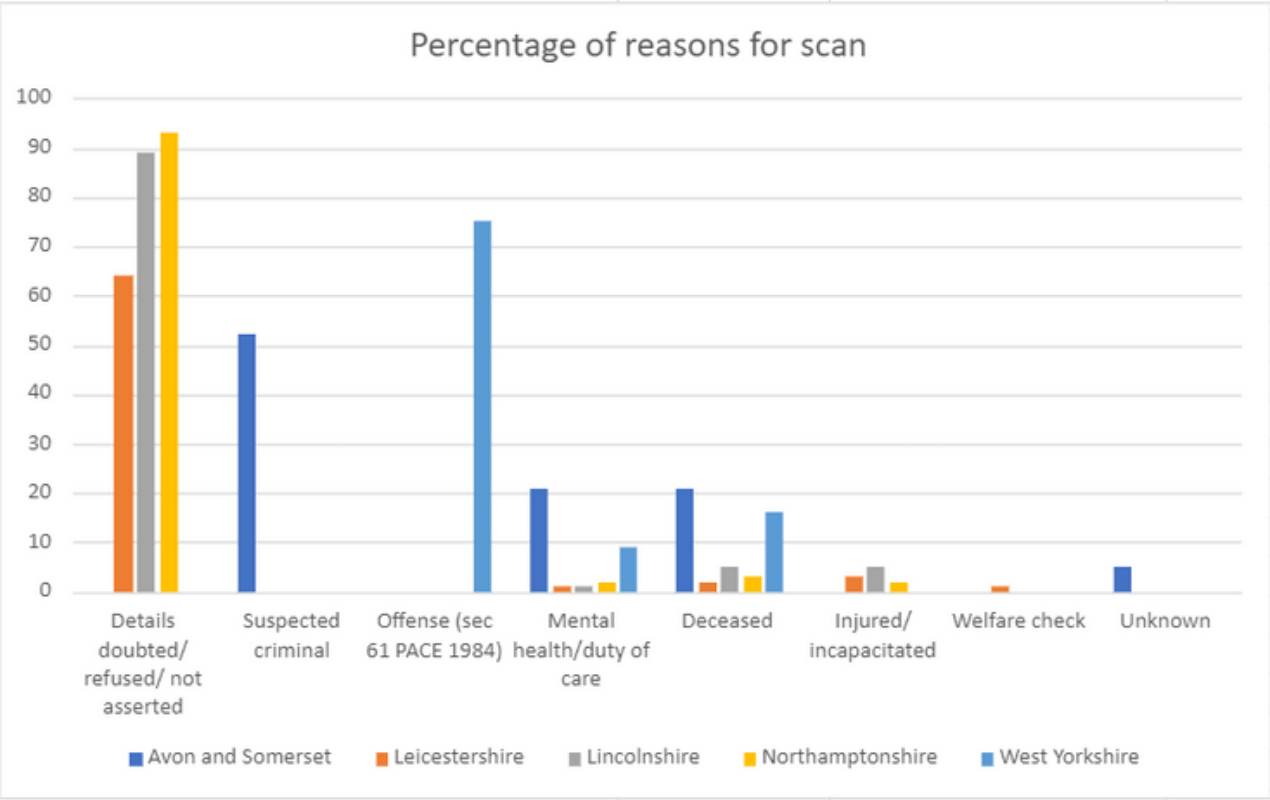
Men are much more likely to be stopped and scanned than women

Reasons for Stop and Scan

Very few police forces disaggregated the reason why they executed a stop and scan. Only five police forces provided data for this question.

Across these five forces, the number one reason provided as to why people are stopped and scanned is because a police officer doubts the details given or the person refused to give their details to the officer. It is not possible to tell from the FOI data what percentage of those are for details doubted and which ones are because the person refused.

In West Yorkshire, most people were scanned for an "offense" under Section 61 of the Police and Criminal Evidence Act. The number of scans carried out because of mental health, because the individual was injured or because the police were conducting a welfare check was significantly low in comparison to details doubted/refused.



FACIAL RECOGNITION TECHNOLOGY

What is Facial Recognition Technology (FRT)?

"Facial Recognition is a technology capable of comparing a human face from a digital image against a database of faces. It analyses key facial features and generates a mathematical representation of these features. It then compares them against the mathematical representation of known faces in a database, generating possible matches." (South Wales Police, 2021)

Since 2015, special cameras in public spaces have been live scanning millions of people's faces **without their knowledge or consent.** Anyone walking past can have their biometric data snatched and compared to images on a watch list. Watch lists **contain pictures of anyone**, including people not suspected of any crime, and **taken from anywhere** including social media accounts.

South Wales Police and Metropolitan Police introduced facial recognition technology prior to any public or parliamentary debate. It has also been used to monitor protests, football matches and festivals.

Big Brother Watch (2022) found that **over 3,000 people have been wrongly identified** by police facial recognition and that the Met's technology is **87% inaccurate** (2016-2022). In 2018, Big Brother Watch initiated legal action which forced the Met to slow down and develop policies restricting its use. They have since started a Stop Facial Recognition Fund to mobilise nationally and grow pressure in parliament for a Bill banning police use.

In 2020, Liberty client Ed Bridges won the world's first legal challenge to police use of this technology. The Court said that South Wales Police's intrusive and discriminatory facial recognition **violates privacy rights** and **breaks data protection and equality laws** (see Liberty 2022). However, despite the court ruling, a number of police forces have reaffirmed their commitment to FRT. Why should we be concerned?

Racial and sexist bias in FRT algorithms is widely documented.

In 2019, the National Institute of Standards and Technology (NIST) published one of the most comprehensive assessments on this issue to date.* NIST analysed 189 facial recognition algorithms submitted by 99 developers, including major tech and surveillance companies. NIST found the majority were substantially less likely to correctly identify a Black woman than a member of any other demographic. Many were 10 to 100 times more likely to misidentify a Black or East Asian than a white face.

Algorithmic bias has real consequences.

The above implies, for example, that Black people are more likely to be misidentified by police FRT and questioned on the basis of a false alert. According to South Wales Police, "Officers can quickly establish if the person has been correctly or incorrectly matched by traditional policing methods i.e. normally a dialogue between the officer/s and the individual" (see Burgess 2018). Rather than counter-acting racial bias, such methods only open up the process to an additional potential source: the subjective judgement of an individual officer.

Is the solution to make facial recognition "more accurate"?

Increased accuracy would require training the algorithm on a new set of biometric data. This begs several questions. Who is the algorithm being trained on? Is their consent properly informed? Do they know what their data will be used for?

*NIST is part of the US Department of Commerce, but develops internationally recognized research and standards for technology.

How is that data being connected to other forms of surveillance? Do they understand the limitations around the "removal" of data from the neutral nets that form facial recognition algorithms? That what the algorithm "learns" from their data will go on to affect the lives of countless others?

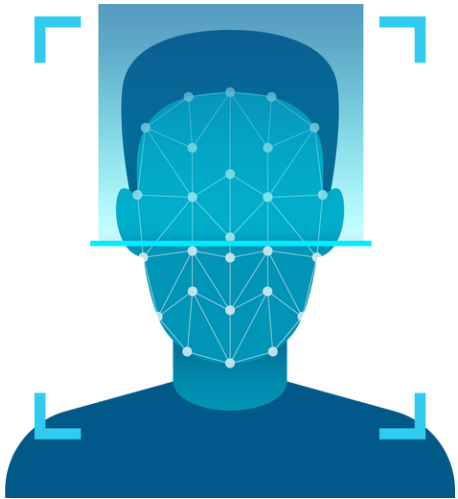
Furthermore, increased accuracy cannot address the way facial recognition is employed to bolster racist surveillance practices. According to Liberty (2022), The Met often deploy FRT in 'ethnically diverse areas and at events highly likely to be attended by people of colour'. In 2017, for example, they piloted FRT software at Notting Hill Carnival - Britain's main annual African-Caribbean celebration.

In other words, our answer is no. Institutional racism exceeds the correction of algorithmic bias.

Operator Initiated Facial Recognition (OIFR) marks the latest evolution of police facial recognition technology.

We are deeply concerned that OIFR is being piloted despite all the above - the 2020 Court ruling, widespread bias with tangible consequences, and evidence of institutional racism in FRT's piloting and deployment.

In the remainder of this report, we focus on the OIFR app currently being piloted. We explain how the app works, how it connects to watchlists and biometric databases, and discuss our findings from Freedom of Information requests sent to the South Wales and Gwent Police Forces.



OPERATOR INITIATED FACIAL RECOGNITION

Operator Initiated Facial Recognition (OIFR) is a mobile phone use of Facial Recognition Technology (FRT) currently being piloted by South Wales Police. It compares a photograph of a person's face taken on a mobile phone to the predetermined watchlist to assist an officer to identify a subject.

In December 2021, South Wales and Gwent Police Forces announced they would begin a pilot scheme using overt facial recognition technology in mobile devices also known as Operator Initiated Facial Recognition (OIFR). The initial number of officers using this technology is 70. The image taken by officers is then compared to Custody images, Missing persons or both data bases. The image, captured on the mobile device, and biometric data are automatically and immediately deleted after a search is carried out.

The Facial Recognition (OIFR) App can be used when:

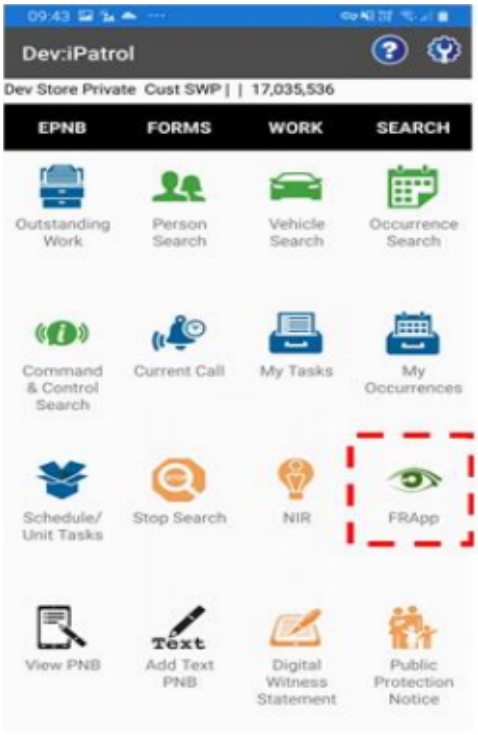
- The subject is unable to provide their details because they are deceased, unconscious, have mental health or age barriers or incapable due to drink or drugs.
- The subject has refused to provide their details
- It is reasonably suspected that the subject has provided false details.

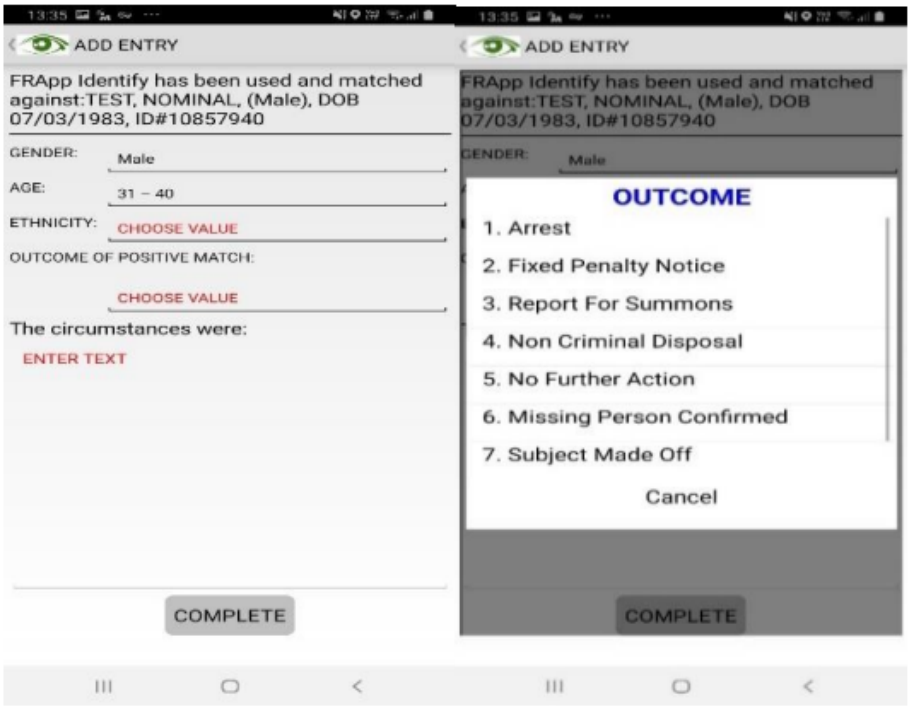
AND when one of the following grounds apply. When the subject is:

- Deceased
- Reported as a missing person

- Suspected to have committed an offence, wanted by the courts, subject to bail conditions or a court order.
- Presenting a risk of harm to themselves or others

OIFR is accessed via the existing iPatrol Application on the Samsung mobile device. Images of the app below obtained via South Wales Police website (2021).





Operator Initiated Facial Recognition (OIFR) app

Phase 1

Stopped by police

Police officers stop person either suspected of committing crime and/or they believe is missing.

Phase 2

Image taken by police

Police officers use their mobile phone to take a picture of the person and compare to watchlists available to police including custody images and missing persons.

Phase 3

Matches made against databases

The technology reorders the chosen watchlist(s) from the most to least likely possible match. The six most likely possible matches are returned to the officer's mobile phone. The officer will review the top six possible matches and decide whether a match has been made. If a match has been made it will then be possible to carry out further checks for the subject against police systems.

Phase 4

Final stage

Possible arrest, fixed penalty notice, report for summons, non criminal disposal, missing person confirmed, subject made off or no further action is taken. Persons who are not included on a watchlist cannot be identified.

KEY FINDINGS OIFR APP

We submitted an FOI to South Wales and Gwent Police in relation to the force's use of overt facial recognition technology in mobile devices also known as Operator Initiated Facial Recognition (OIFR), from December 2021 to March 2022.

Gwent police responded to our FOI stating: "We can confirm that the Operator Initiated Facial Recognition app is not used within Gwent Police due to technical issues."

Number of times OIFR was used

South Wales police stated OIFR was used 42 times on 35 different subjects within the requested time frame.

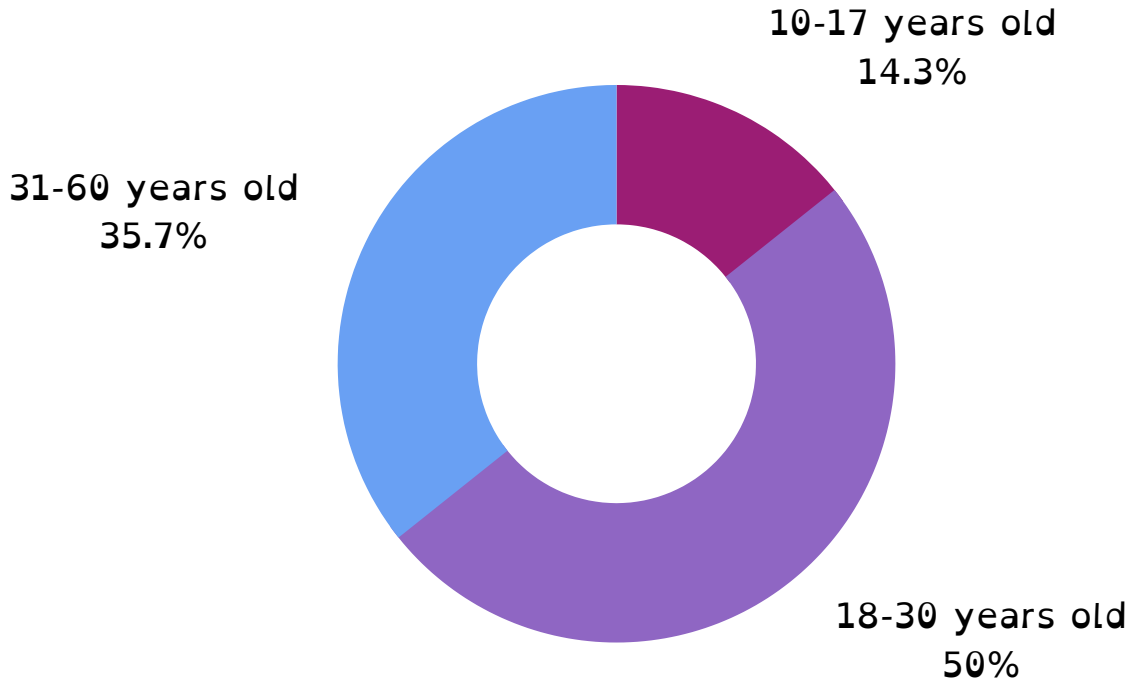
Database used

Ident1 and IABS are not integrated into the OIFR App. Details of Police National Computer (PND) searches are not recorded.

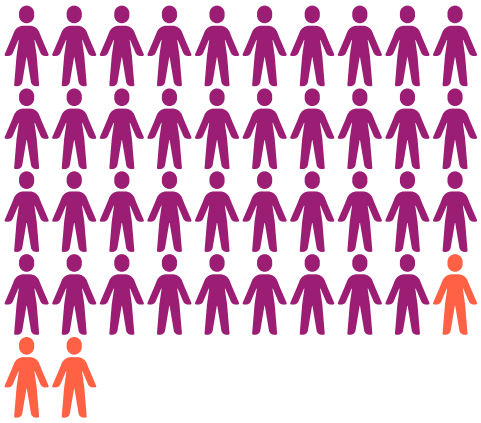
Any records documenting the rate of false positives and false negatives.

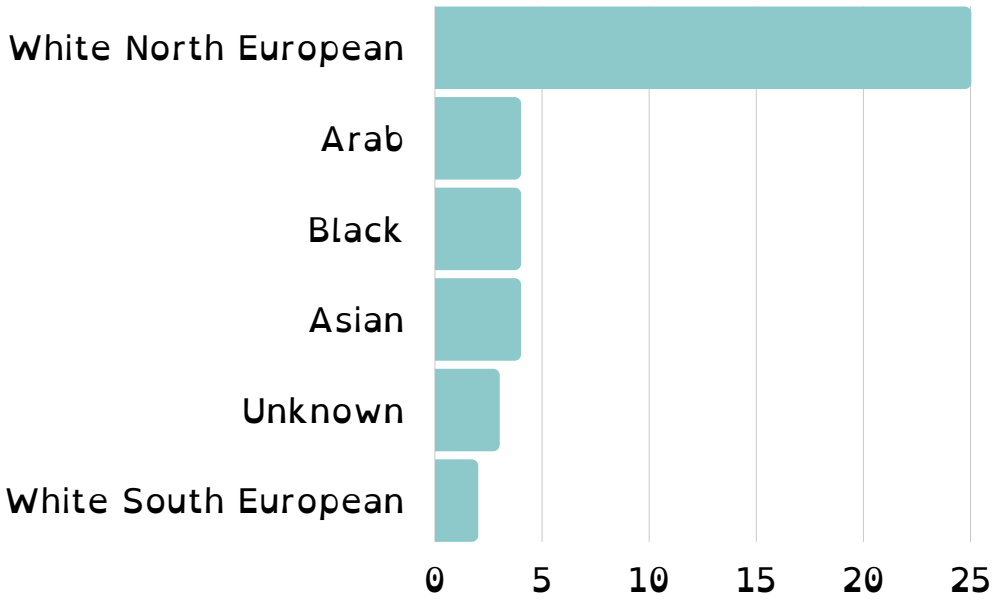
Unlike Live facial recognition the user is not presented with one potential match they are presented with six suggestions. South Wales police said they "are confident that no one was incorrectly identified as a result of OIFR use". Yet, it is not clear how they came to this determination as it depends on the police officer to ascertain if the search turns a match given the six options via the app.

Percentage of Face Scans According to Age



39 face scans on men, compared to 3 on women.





Number of Face Scans According to Ethnicity

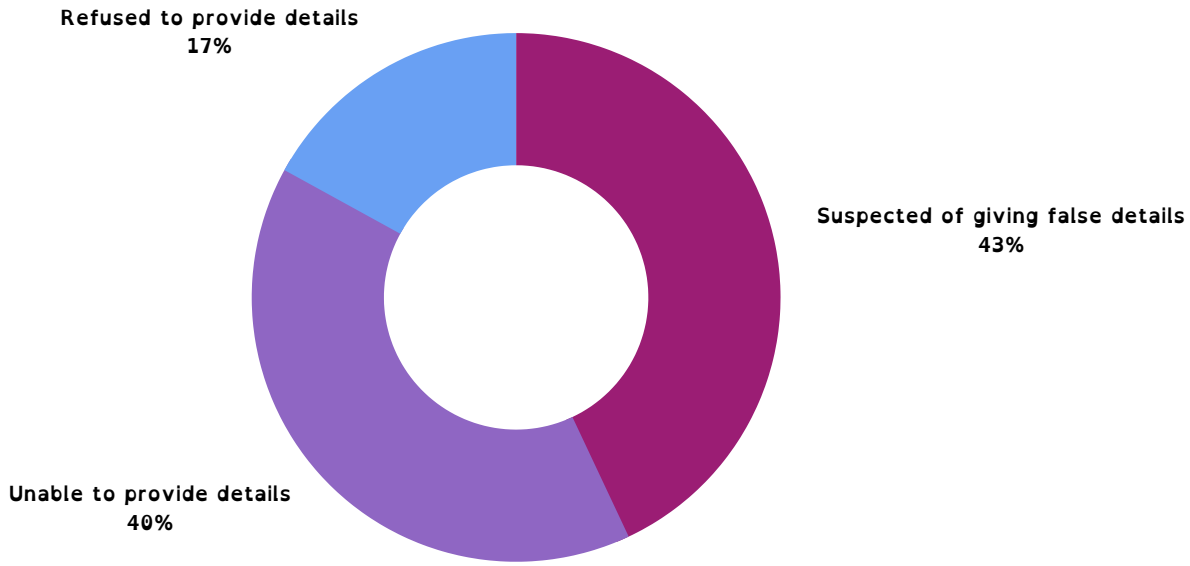
Reason for Stop and Face Scan	Grounds for Face Scan	Database Searched	Outcome of Scan
7 people refused to provide details	6 people were suspected of committing an offense 1 person suspected of being missing	3 custody 4 both missing person and custody	3 arrests 3 no further action 1 abandoned female refused to consent
18 people were suspected of giving false details	15 people were suspected of committing an offense 3 people were suspected of being a missing person	8 custody 10 both missing person and custody	6 arrests 5 no further action 3 report for summons 2 incomplete 1 non criminal disposal 1 missing person
17 people were unable to provide details	9 people were suspected of committing an offense 5 people were suspected of being missing 2 people were deceased 1 person was suspected to suffer harm	5 custody 11 both missing person and custody 1 missing person	2 arrests 8 no further action 3 deceased 1 report for summons 1 non criminal disposal 2 non specified

Reason for Stop and Face Scan	Grounds for Face Scan	Database Searched	Outcome of Scan
TOTAL OF 42 STOPS* ***OF 35 SUBJECTS. SOME WERE STOPPED TWICE.**	30 suspected of a crime 9 missing people 2 deceased 1 suspected to suffer harm	25 both 16 custody 1 missing person	16 no further action 11 arrests 4 report for summons 3 deceased 2 non criminal disposal 2 non specified 2 incomplete 1 missing person 1 refused

Our findings reflect concerns that this technology is primarily used on grounds of 'suspicion' and thus subject to misuse and racial profiling. Of the total number of stops (rather than subjects):

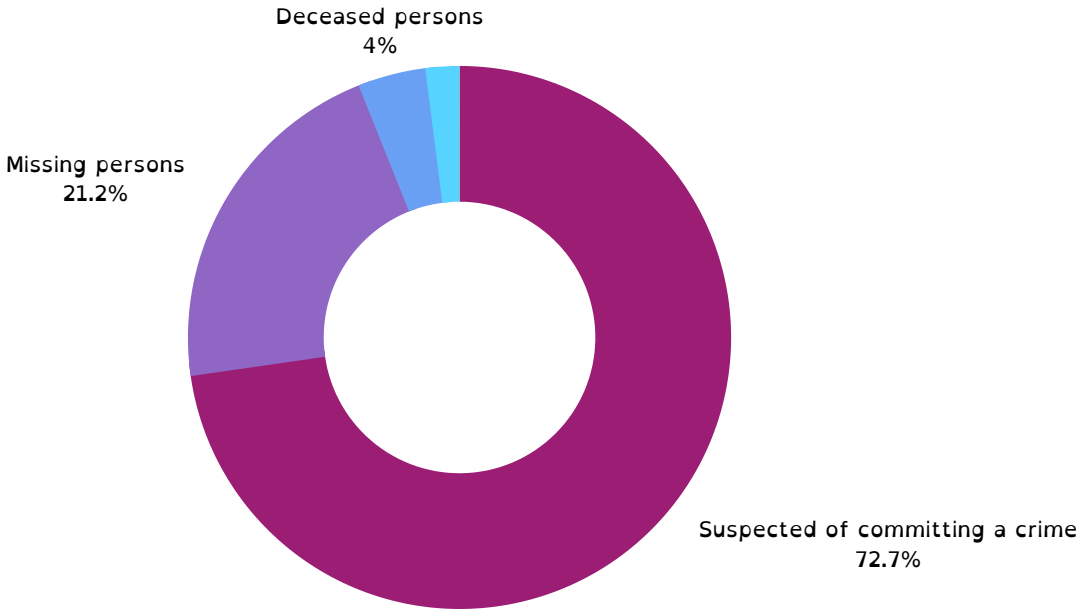
- 43% were scanned when suspected of giving false details, closely followed by 40% when unable to provide details. Only 17% refused to provide details.

Reason for Stop and Face Scan



- 72% were scanned when suspected of committing a crime. 21% were scanned on missing person grounds. Only 4% on deceased grounds, and 2% because they were suspected to suffer harm.

Grounds for Face Scan



Finally, of these total number of face scans (not subjects):

- 60% of people scanned were searched against both the Custody and the Missing Person database. 38% were exclusively against the former and only 2% exclusively against the latter.

- 37% resulted in no further action. However, 26% resulted in arrest and 10% in summons to court for prosecution ("Report for Summons"). 4% resulted in the issuing of some form of non criminal disposal (e.g., cautions and warnings). The remaining 21% were labelled either 'Deceased', 'Non Specified', 'Incomplete', 'Missing Person' or 'Refused' in the FOI data.

RECOMMENDATIONS

01 — Stop using technology

The use of mobile fingerprint scanners and facial recognition software should immediately cease. It disproportionately is used on racially minoritised communities and does not help in keeping our communities safe. It is also an encroachment on our privacy.

02 — Firewall

Police officers should have no direct link to the immigration database. Mistakes have consistently been found in immigration information putting people being stopped and scanned in very vulnerable situations.

03 — Migrants deserve data protection

Remove "immigration control" exemption in Schedule 2, Part 1, paragraph 4 of the Data Protection Act 2018, which allows data processors to set aside an individual's GDPR data protection rights if fulfilling those rights would prejudice "the maintenance of effective immigration control" or "the investigation or detection of activities that would undermine the maintenance of effective immigration control."

04 — Fund community and grassroot initiatives

Fund community advocates and grassroots organisations who are supporting racially minoritised individuals and migrant communities, particularly if they have been victims of hate crimes or state oppression.

RECOMMENDATIONS

05 — Implement reviews

Police forces must implement recommendations from the MacPherson report to address institutional racism as well as the suggestions made in Liberty and Southall Black Sisters' police super complaint.

The Home Office must apply the recommendations made by the Windrush Lessons Learned Review. See also RJN's (2020) Hate Crime report on ways to address the intersection of crime and migrant oppressions.

06 — End Hostile Environment

End Hostile Environment policies which disproportionately affect Black and Brown migrant communities. These policies exacerbate existing inequalities and enforce material and emotional violence in our communities.

07 — End Stop and Search

Stop and search tactics are disproportionately used on racially minoritised communities, particularly Black young men. These tactics do not help keep our communities safe. Rather, they cause irreparable harm to our loved ones.

REFERENCES

BBC London (2019) 'This Gadget Means Police Can ID You Anywhere' 12th October 2019. YouTube [online video] Available at: https://www.youtube.com/watch?v=Ladzel6BA4U

Big Brother Watch (2022) 'Stop Facial Recognition'. Big Brother Watch [online] Available at: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#fund

Burgess M (2018) 'Facial Recognition Tech Used by UK Police is Making a Ton of Mistakes' 4th May. Wired [online]. Available at: https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival

Liberty (2022) 'Facial Recognition'. Liberty [online]. Available at: https://www.libertyhumanrights.org.uk/fundamental/facial-recognition/

Liberty and Southall Black Sisters (2022) LIBERTY AND SOUTHALL BLACK SISTERS' SUPER-COMPLAINT ON DATA-SHARING BETWEEN THE POLICE AND HOME OFFICE REGARDING VICTIMS AND WITNESSES TO CRIME, https://www.libertyhumanrights.org.uk/issue/liberty-and-southall-black-sisters-super-complaint-on-data-sharing-between-the-police-and-home-office-regarding-victims-and-witnesses-to-crime/

The Racial Justice Network (2020) Hate Crime & System(ic) Injustice: a Report on the Experiences of Reporting Hate Crime in West Yorkshire. The Racial Justice Network, https://racialjusticenetwork277579038.files.wordpress.com/2020/11/hate-crime-and-systemic-injustice-a-report-by-the-racial-justice-network-1.pdf

REFERENCES

The Racial Justice Network and Yorkshire Resists (2021) 'Public's Perception on Biometric Services Gateway (mobile fingerprint app), UK.' The Racial Justice Network, https://racialjusticenetwork277579038.files.wordpress.com/2021/01/report-public-perception-biometric-gateway.pdf

South Wales Police (2021) 'Facial Recognition Technology'. South Wales Police [online]. Available at: https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/

Step Up Migrant Women, https://stepupmigrantwomen.org/

Stop the Scan (2020) Stop the Scan – Stop UK Police Scanning Biometrics for Home Office Border Enforcement. Stop the Scan [online video]. Available at: https://stopthescan.co.uk/

Wangari-Jones P, Loyola-Hernández L, and Humphris R (2021) 'STOP THE SCAN: Police Use of Mobile Fingerprinting Technology for Immigration Enforcement, UK'. Racial Justice Network and Yorkshire Resists, https://racialjusticenetwork277579038.files.wordpress.com/2021/06/stop-the-scan-report.pdf

SUPPORT STOP THE SCAN

Sharing our content via social media and with your wider networks always helps! Tag us using our social media and the hashtags #StopTheSCANdal #HandsOffOurPrints and #HandsOffOurBiodata

We welcome donations of any kind. You can donate via RJN website.

If you have skills, networks or other ideas to support our campaign get in touch via email at stopthescan@racialjusticenetwork.co.uk or info@racialjusticenetwork.co.uk

Finally, we are always looking for volunteers from diverse backgrounds to be part and support RJN and Yorkshire Resists. You don't have to be based in West Yorkshire.

If you have been stopped and scanned please contact us at stopthescan@racialjusticenetwork.co.uk

The Racial Justice Network

registered charity no. 1165804
Bread and Roses, 14 North Parade, Bradford, BD1 3HT
+44 7592160352 |
+44 7542876043

www.racialjusticenetwork.co.uk

@RaceJustice

@theracialjusticenetwork

Yorkshire Resists

www.stopthescan.co.uk

@YorksResists

@yorkshireresists