



BIOMETRIC BRITAIN:

The Expansion of Facial Recognition Surveillance



About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Silkie Carlo

Director

Email: silkie.carlo@bigbrotherwatch.org.uk

Jake Hurfurt

Head of Research and Investigations

Email: jake.hurfurt@bigbrotherwatch.org.uk

Madeleine Stone

Legal and Policy Officer

Email: madeleine.stone@bigbrotherwatch.org.uk

Biometric Britain: The Expansion of Facial Recognition Surveillance

Published: 23/05/23

Contents

INTRODUCTION.....	1
RECOMMENDATIONS.....	4
WHAT IS FACIAL RECOGNITION TECHNOLOGY?.....	6
PUBLIC SECTOR FACIAL RECOGNITION.....	8
POLICE LIVE FACIAL RECOGNITION.....	9
<i>How Does It Work?</i>	9
<i>Where is LFR Used?</i>	12
<i>On The Ground At Deployments</i>	15
<i>Signage Requirements</i>	15
<i>The Right to Refuse</i>	16
<i>Proving Innocence</i>	17
<i>Watchlists</i>	17
<i>Use Statistics</i>	20
<i>Policy Analysis</i>	22
Commentary from Dr Ed Bridges.....	28
POLICE RETROSPECTIVE FACIAL RECOGNITION.....	30
<i>What is RFR?</i>	30
<i>Who Uses RFR?</i>	31
<i>How is RFR Used?</i>	31
<i>Statistics</i>	37
POLICE NATIONAL DATABASE FACIAL SEARCH.....	39
<i>What Is the PND?</i>	39
<i>How Does Facial Searching Work?</i>	39
<i>How Many Images Are On It?</i>	40
<i>Unlawful Retention of Custody Images</i>	40
<i>Policy Analysis</i>	43
<i>Risk to privacy</i>	43
<i>Lack of legal basis</i>	44
HOME OFFICE BIOMETRICS PROGRAMME.....	47
POLICE OPERATOR INITIATED FACIAL RECOGNITION.....	49
<i>Who Uses OIFR?</i>	49
<i>How is OIFR Used?</i>	49
<i>Image Reference Database</i>	55
<i>Use Statistics</i>	56
<i>Comparison to Other Street Biometrics</i>	60
<i>Policy Analysis</i>	61
KEY UK REPORTS AND RULINGS.....	64
<i>Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology 2019</i>	64

<i>R (Bridges) v South Wales Police, Court of Appeal Ruling, 2020</i>	66
<i>Equitability Study, National Physical Laboratory, 2023</i>	67
FACIAL RECOGNITION IN SCHOOLS.....	71
<i>Case Study</i>	73
Commentary from Jen Persson, Defend Digital Me.....	76
FACIAL RECOGNITION IN VISAS & IMMIGRATION.....	77
<i>EUSS</i>	77
<i>Right To Work</i>	79
<i>Commentary from Dr Laura Loyola-Hernández, Yorkshire Resists</i>	81
PRIVATE SECTOR FACIAL RECOGNITION	83
PIMEYES.....	84
<i>What Is PimEyes?</i>	84
<i>Traumatic Images</i>	85
<i>Cyberstalking</i>	87
<i>Children</i>	88
<i>User Suggestions</i>	89
<i>Big Brother Watch Complaint</i>	90
CLEARVIEW AI.....	92
<i>How It Works</i>	92
<i>Who Uses It</i>	93
<i>ICO Ban in the UK</i>	93
<i>Policy Analysis</i>	94
<i>Commentary from Cher Scarlett</i>	97
FACEWATCH.....	98
<i>How Does It Work?</i>	99
<i>The Watchlist</i>	100
<i>Facial Matching & Alerts</i>	101
<i>Non-Retail Uses</i>	102
<i>Policy Analysis</i>	103
CASINOS & GAMBLING.....	106
<i>Bookmakers</i>	106
<i>Casinos</i>	106
FACIAL RECOGNITION AS A CCTV CAMERA CAPABILITY.....	109
<i>Hikvision and Dahua</i>	109
CONCLUSIONS	111
APPENDIX – POLICE LFR DEPLOYMENT DATA SINCE 2019	113

“The boom in facial recognition technology in the UK, operating in a largely lawless space, is a mortal threat to privacy as we know it. Walking down the street anonymously could soon be a thing of the past if the spread of live facial recognition is not resisted”

Introduction

The expansion of Orwellian facial recognition technology in the UK has continued at an alarming pace since Big Brother Watch's first report on face scanning cameras, *Face Off: The Lawless Growth of Facial Recognition in UK Policing*, was published in May 2018.

Our report sparked a national conversation and the Metropolitan Police committed to pursue no more than 10 "trial" deployments that would be subjected to an independent review, before making a decision as to whether to operationally deploy the technology. The highly unusual "trials" had no set parameters for failure or success, no time frame, consisted entirely of operational deployments, and cost the taxpayer millions of pounds. The resulting independent review was damning, finding that 81 per cent of the people flagged by live facial recognition were in fact innocent people who had been misidentified, and that it was "highly possible" that the Metropolitan Police's use of the surveillance technology would be found to be unlawful if it were challenged in court.¹ Meanwhile, campaigner Dr Ed Bridges brought a landmark legal challenge against South Wales Police's use of live facial recognition surveillance, which had included a deployment at an anti-arms fair protest in which every person on the watchlist was innocent and not wanted by police, and won in the Court of Appeal which found that the force's use of the technology had been unlawful.²

Despite the serious accuracy and legal issues, both the Metropolitan Police and South Wales Police have continued to deploy live facial recognition in London, Cardiff and Swansea. The deployments turn our city streets into mass-scale police line-ups with hundreds of thousands of innocent people subjected to biometric identity checks. Despite scanning more than 560,000 people, the equivalent of the population of Belfast over the past five years, only 57 people were correctly identified while the technology got it wrong 90 times.³

Seven years after UK police first rolled out this invasive technology there has still been no democratic consent to live facial recognition biometric surveillance in Britain. No legislation has been passed, or even seriously proposed to approve or ban the use of live facial recognition technology in the UK. Instead, police operate in a grey area enabled by a democratic deficit to use rights-invading technology with minimal oversight.

1 Independent Report On The London Metropolitan Police Service's Trial Of Live Facial Recognition Technology, Professor Peter Fussey and Dr Daragh Murray, Human Rights, Big Data and Technology Project, University of Essex, July 2019, <https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf>

2 R (Bridges) v The Chief Constable of South Wales Police, Court of Appeal (Civil Division). EWCA Civ 1058, 11th August 2020, <https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf>

3 The real number of faces scanned is likely to be even larger than the c.560,000 known as many deployments from both the Metropolitan Police and South Wales Police did not report the number of faces seen by the cameras.

Subsequent to our 2018 report, several critical reports calling for heavy restrictions or bans on the use of LFR citing privacy and discrimination concerns. Despite a two year pause on live facial recognition deployments in 2020-2, police forces have ignored many of these concerns and resumed using LFR. Recently, they commissioned a government report purporting to address concerns about the bias in the facial recognition algorithm, claiming the racially disproportionate inaccuracy can be mitigated by using accuracy settings above those that have been used operationally.

Over the past five years, police have invested in even more forms of facial recognition technology, including retrospective and operator initiated. Both tools rely on huge custody image databases which contain thousands of photographs that police have retained unlawfully. Yet instead of ensuring they comply with the law, police forces claim that it is too time-consuming to delete these unlawfully held photographs and continue to use innocent people's faces in their biometric databases.

The increasing use of retrospective facial recognition by police forces presents some major risks to privacy and civil liberties, and could see innocent people having to prove they are not who the technology claims they are, while operator-initiated [mobile phone-based] facial recognition threatens to equip police with invasive biometric scans on demand.

Facial searching on the Police National Database, which was found to perform poorly a in Home Office-run study, has almost the exact same set of problems around the unlawful use of images as in the 2018 Face Off report – showing how police have sought to expand their biometric capabilities while doing little to protect individual data rights over the past five years.⁴

Other parts of the public sector have also tried to introduce biometric face scanning, with schools using coronavirus as an excuse to replace lunch cards with face-scanning tills for children, and the Home Office making facial recognition the key to its scheme to process millions of claims for residency in the UK following Brexit.⁵

The private sector has also capitalised on the growth of cheap and easy-to-use facial recognition algorithms, building and selling intrusive surveillance tools that put everyone's privacy at risk. Retailers can now pay a small fee to have facial recognition cameras fitted on their doors to alert staff to "undesirables", giving corner shops access to national facial recognition networks that even the police would be envious of.

Numerous companies are making attempts to become Google for faces. Clearview [now banned in the UK] has become a de-facto privatised law enforcement tool. US police forces alone have made more than a million searches against a database of 30 billion

4 Use Of Facial Recognition Tech 'dangerously Irresponsible', BBC News, 13th May 2019

5 Facial Recognition In Our Schools, Leverhulme Academy Trust, accessed 20th March 2023, <https://www.leverhulmeacademytrust.org/Facial-Recognition/>

photos - more than three for every single person on the planet and all collected from every corner of the internet without the subject's knowledge or consent. Meanwhile, PimEyes offers similar services to consumers; it claims to be a privacy-focussed tool individuals can use to find pictures of themselves online, but in reality, it has facilitated the stalking and harassment of women online and allows users to track almost anyone. Action against facial search engines must be taken quickly to halt their lawless growth, which could erode anonymity forever.

The boom in facial recognition technology in the UK, operating in a largely lawless space, is a mortal threat to privacy as we know it. Walking down the street anonymously could soon be a thing of the past if the spread of live facial recognition is not resisted, while the central government is working to create a mega-database of biometrics that could be instrumentalised against migrant communities, and to discriminate against ethnic minorities.

Big Brother Watch has been tirelessly fighting against the growth of facial recognition surveillance since its foundation and particularly since our 2018 report. Our presence at police deployments of LFR has acted as a check on early uses of the surveillance technology in London and Cardiff, while we have launched complaints and challenges against facial recognition across the private sector, from Clearview and PimEyes to Facewatch.

This report consolidates our research on the expansion of facial recognition in the UK since we published our 2018 Face Off report five years ago, and highlights the ethical, legal and human rights threats it poses. We make a series of policy recommendations to better protect privacy, equality and the rights threatened by unrestrained facial recognition surveillance.

Recommendations

Live Facial Recognition

RECOMMENDATION: The use of live facial recognition by police forces and private companies for public surveillance must be immediately stopped in the UK.

Retrospective Facial Recognition

RECOMMENDATION: There is currently no evidence base, nor a clear and sufficient legal framework, for the use of RFR. If police make a strong business case for the strict necessity of RFR, the Government should consider it and, before any operational use of RFR, introduce new primary legislation in order to bring in the safeguards and restrictions on the use of RFR as outlined in the recommendations in this report.

RECOMMENDATION: In recognition of the intrusive nature of retrospective facial recognition, police should have limitations on the circumstances in which it can be used. A biometric search should only be undertaken when strictly necessary to identify an individual in the image is suspected of carrying out a qualifying offence, as defined by Section 65A of the Police and Criminal Evidence Act 1984.

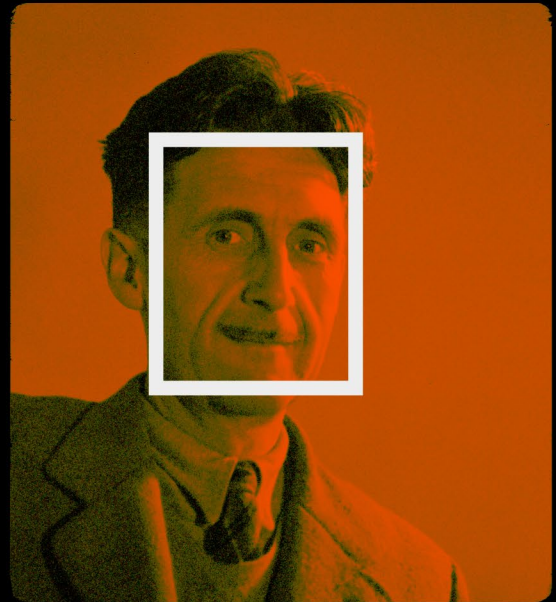
RECOMMENDATION: The Home Office must work with police forces to ensure the automatic deletion of the thousands of images of unconvicted individuals from the Police National Database and police force databases. Police forces should only be permitted to carry out retrospective facial recognition searches on lawfully held custody images.

RECOMMENDATION: Police forces must respect the privacy rights of individuals when sourcing probe images. Probe images from non-police originated sources should be collected and processed only where police originated images are unavailable.

Operator Initiated Facial Recognition

RECOMMENDATION: The use of operator-initiated facial recognition by police forces should be prohibited as no case has been made as to why such power is strictly necessary and it poses a significant risk to the rights of the British public. Individuals can be identified at police stations if there is a lawful reason for their arrest.

Detection



Facial
analysis



Identification



What is Facial Recognition Technology [FRT]?

Facial recognition technology seeks to leverage the uniqueness of human facial features either for surveillance or to match/identify individual faces. It works through software which measures and analyses a face's particular characteristics to create a unique biometric template, or map, of that face which is then converted to a string of numbers [a code]. Algorithms then compare these codes to a database or watchlist, made up of other face maps, to search for potential matches.

Unlike facial recognition tools seen in films or television, FRT produces a match score, usually a percentage, that rates the similarity of the facial image with others on the database. Depending on the tool used and confidence settings there may be one or a handful of potential matches generated by the system.

The process can be split into three main stages:⁶⁷

- **Detection:** The software detects the presence of a face, or faces, in an image.
 - (a) Mobile phone cameras which focus on a face, or screens relaying feeds from CCTV cameras that place boxes around faces use a similar process
- **Facial analysis:** The software analyses a face's unique features, such as the shape of a person's cheekbones, the space between their eyes [known as interocular distance] or the depth of their eye sockets. Algorithms then convert this into a unique map, or string of numbers, known as a faceprint.
 - (a) These numerical strings can theoretically be reverse-engineered to produce an approximation of the face that was analysed to generate it.
- **Identification:** FRT technology cross-references the faceprint against a database, which could be very small or very large, and produces a list of likely matches that are above the similarity score threshold in the system.
 - (a) The outcome then varies depending on the purpose of the system: for example, a mobile phone security FRT system would then unlock the device or not depending on the result whereas a police system may then alert officers of a likely match to somebody on the watchlist.

Facial recognition can work on a one-to-one basis, which is often for identity verification, or a one-to-many [1:N] basis, which is often used for identification. Verification requires a

6 How Facial Recognition Works, The New York Times, 15th July 2020, <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>

7 What is Facial Recognition, Amazon AWS, accessed 14th February 2023, <https://aws.amazon.com/what-is/facial-recognition/>

template to be chosen before authentication. One example may be if a gym user swipes a membership card and then undergoes facial recognition to match their appearance against a pre-enrolled photograph associated with the card – here the faceprint is being compared with a single record. Identification, or a 1:N system, sees a faceprint compared with a database of other prints to search for potential matches. It is the latter system that is mostly addressed in this report as it is identification, rather than verification, which is more at risk of use for mass surveillance.

The technology can be deployed in several different ways, depending on the use case and reference database, but the main types in use in the UK are:

- **Live Facial Recognition** – Real-time analysis of CCTV feeds where the software analyses faces passing by the camera instantaneously, effectively acting as an identity check for anyone walking past the FRT set-up.
- **Retrospective Facial Recognition** – The application of FRT to recorded video or pictures post-event, comparing faces in the images against a watchlist or even entire police databases.
- **Operator-initiated Facial Recognition** – Mobile phone-based on-demand facial recognition, where users capture a facial image which is then compared against a database.
- **Verification** – Comparing a face photograph against a pre-enrolled image to verify someone's identity, such as a phone being unlocked with facial recognition or the matching of an ID to an individual.

Public Sector Facial Recognition



Live Facial Recognition

Live Facial Recognition [LFR] is a form of automated facial recognition which operates near-instantaneously. The software analyses live video feeds to recognise and match faces against a watchlist. Both the Metropolitan Police in London and South Wales Police have used LFR over the past five years, moving from so-called “trials” to active deployments.

LFR is perhaps the most intrusive form of automated facial recognition technology as it is used to indiscriminately scan anyone passing by the camera in a public space, often without their knowledge. The streets where LFR is deployed become de-facto police line-ups, where everyone is a potential suspect. In a policing context it is used in combination with a deployment of officers who seek to intervene with any potential matches amongst a crowd at that moment.

How Does It Work?

Police can feed almost any live video recording into the facial recognition software to scan the faces of passers-by and compare them against a watchlist in real time - effectively, it works as an identity check for anyone seen by the camera.

Deployments in the UK have usually involved dedicated cameras connected to nearby servers running the recognition algorithms – most often a CCTV van with computers inside, but this is not a necessary condition of LFR. With high-speed internet and high-resolution surveillance cameras, it is plausible that police could tap into an internet stream of a far-away camera and analyse it with the software.

The Metropolitan Police outlines a six-stage process for the actual operation of LFR:⁸

1. A watchlist is compiled using images from existing databases
 - a) These images are processed by the FR software to generate the mathematical “faceprints” to compare the probe images to
2. Facial images are acquired
 - a) A camera or cameras monitor a public space and capture a live video feed of people passing by
3. Face detection
 - a) The LFR software detects the human faces in the video feed

⁸ Live Facial Recognition Policy, Metropolitan Police, accessed 30th March 2023, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document.pdf>

4. Face extraction
 - a) The software extracts the facial features from detected faces and converts them to a biometric template, or "faceprint"
5. Face comparison
 - a) The faceprints are compared with those held on the watchlist
6. Matching
 - a) As the faceprints are compared the software generates a numerical similarity score to indicate how similar a captured facial image is to any face on the watchlist. Police set a "threshold" for these scores, above which potential matches are flagged as an alert for officers to view and act on if necessary.

Once the LFR process itself is complete it is up to police officers involved in the deployment to decide how to interact with anybody flagged as a potential match, from deciding whether the alert is indeed the person the system thinks it may be to intervening and any further police action.

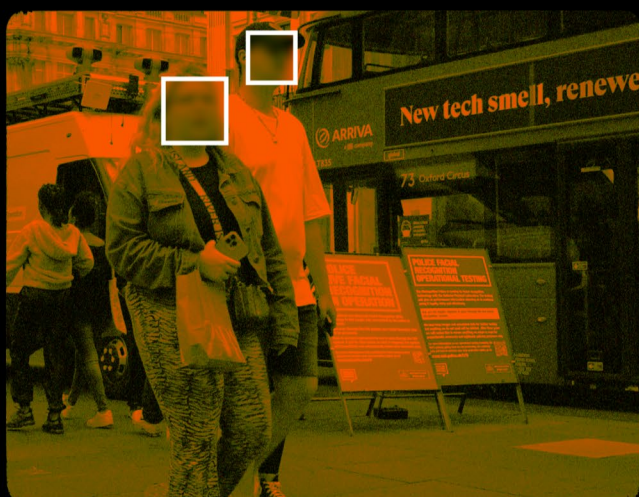
Watchlist compiled



Facial images acquired



Face detection



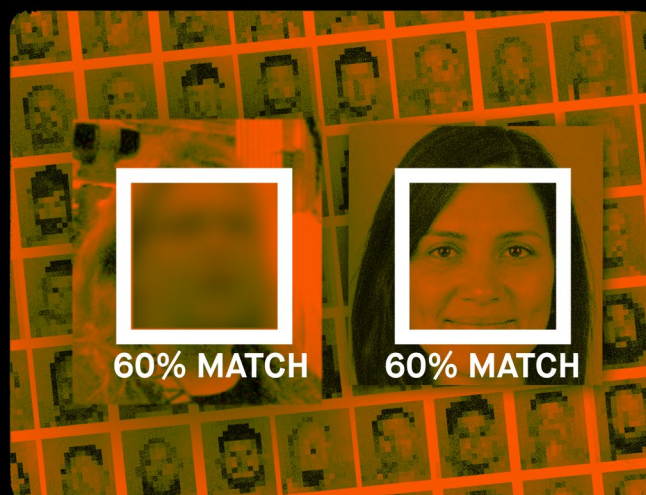
Face extraction



Face comparison



Face matching



Where is LFR Used?

Only two UK police forces, the Metropolitan Police and South Wales Police, overtly use live facial recognition regularly. Both forces have deployed LFR in public spaces with high footfall and both have roughly equivalent procedures for where and when they deploy LFR.

LFR has been used predominantly in busy city centre locations in London, while in South Wales LFR has been focussed on major events such as sports games and concerts.⁹

Examples of the specific locations LFR has been deployed include:

- Westfield Shopping Centre in Stratford
- Oxford Circus, London
- Leicester Square, London
- Romford High Street
- Notting Hill Carnival
- Six Nations Rugby matches [Wales v Italy at the Principality Stadium on 21/03/2022]
- Swansea City v Cardiff City [both home and away fixtures in the 2019/20 season]
- Slipknot concert at the Motorpoint Arena
- Spice Girls concert at the Principality Stadium

Police documents state that LFR deployment locations should be places where there are “reasonable grounds” to suspect one or more people on the watchlist will be present during the time frame of the deployment.¹⁰ The Met states that location selection might be supported by intelligence about said location, including any perceived public safety risk. Police are also required to consider the public’s expectation of privacy at a proposed deployment location – for example, the Met views this expectation as being higher in a quiet suburban park than on a busy street in central London.

Certain types of locations also come with a higher expectation of privacy, as do places where there is a risk of LFR interfering with other rights, including free expression, when considering where to deploy facial recognition. These include hospitals, places of worship, schools and protests.¹¹ Although police are required to weigh up the expectation of privacy against the claimed necessity of deploying LFR for policing purposes, the justification for any particular location is rarely made public.

⁹ Stop Facial Recognition, Big Brother Watch, accessed 30th March 2023, <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>

¹⁰ Standard Operating Procedure for Live Facial Recognition, Metropolitan Police, accessed 30th March 2023, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-sop.pdf>

¹¹ Standard Operating Procedure for Live Facial Recognition, South Wales Police, accessed 30th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/live-facial-recognition/lfr-sop-v1.1.pdf>

In one heavily-redacted document obtained by Big Brother Watch about a trio of 2022 LFR deployments on the corner of Oxford Street and Regent Street in central London, the Metropolitan Police discussed the West End's reputation as a destination for shopping, dining and nightlife – and the attraction the area has to criminals. The document, an application for authorisation to deploy LFR, also claimed that the significant CCTV surveillance in the proposed location lessens the expectation of privacy in the area.¹² However, significant amounts of the document are redacted meaning it offers limited additional insight into the choice of location by the Metropolitan Police.

Following the publication of its equitability study in April 2023 the Metropolitan Police deployed LFR three times in Camden and Islington to little success. It also used LFR at the coronation of King Charles III in at least two different locations. The coronation deployment, for which figures are pending as this report is published, could end up being the biggest LFR deployment in UK history given the multiple locations and sheer size of the crowds in central London on the day.

Some older deployments by both forces also have particularly worrying community contexts, both for the groups impacted and the nature of the events targeted by LFR.

In 2016 and 2017 the Met Police used LFR at Notting Hill Carnival, the largest African-Caribbean event in the country. More than 500 people were on the watchlist, but 2016 saw one false match and zero true ones, while 2017 saw 95 false matches and just a single true one.¹³ Targeting community-based events with mass biometric surveillance, especially when the same communities are harmed by the Met's institutional racism¹⁴, underlines how this technology could be used to the detriment of particular groups.¹⁵

The potential for certain demographics or groups to be targeted is an ongoing concern with facial recognition.

South Wales Police had previously targeted a protest with LFR in 2019. The Welsh force deployed facial recognition at a demonstration outside an arms fair at the Cardiff International Arena in 2017.¹⁶ It was this deployment that led to the landmark Court of Appeal Judgement *R (Bridges) v South Wales Police*, where the court held that the force's

12 LFR Application, Freedom of Information Request to the Metropolitan Police, FOI22/026317, 30th November 2022

13 Freedom of Information Request to the Metropolitan Police, FOI2018040001107, 25th April 2018, <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Metropolitan-Police-2018040001107.pdf>

14 An Independent Review Into The Standards Of Behaviour And Internal Culture Of The Metropolitan Police Service, Baroness Casey of Blackstock DBE CB, March 2023, <https://www.met.police.uk/SysSiteAssets/media/downloads/met/about-us/baroness-casey-review/update-march-2023/baroness-casey-review-march-2023.pdf>

15 An Independent Review Into The Standards Of Behaviour And Internal Culture Of The Metropolitan Police Service, Baroness Casey of Blackstock DBE CB, March 2023, <https://www.met.police.uk/SysSiteAssets/media/downloads/met/about-us/baroness-casey-review/update-march-2023/baroness-casey-review-march-2023.pdf>

16 Facial Recognition: What Led Ed Bridges To Take On South Wales Police, 11th August 2020, <https://www.bbc.co.uk/news/uk-wales-53742099>

use of facial recognition was unlawful and breached Dr Ed Bridges' rights.¹⁷

The use of LFR against peaceful protesters is a particularly concerning scenario where biometric scans could be used against people exercising their political rights, engaging Articles 10 (freedom of expression) and 11 [freedom of assembly] of the Human Rights Act. Dr Bridges, who has written a contribution to this report, expressed concern that the use of LFR would impact an individual's right and willingness to protest. Although LFR has not since been used at protests, in documents relating to operator-initiated facial recognition the future possibility has been raised [this is outlined in the section on OIFR], and the risk this poses to protest rights remains.

Facial recognition has also been deployed by the police, or with their approval, at a number of busy publicly accessible but privately owned places.

This included Granary Square, near Kings Cross Station in central London where the private company running the space was passed seven photos by the police so they could place individuals on their facial recognition watchlist.¹⁸ Granary Square used facial recognition in total secrecy for two years and had an agreement with local police to share images. However, after initially denying any knowledge of the LFR use at Kings Cross, the Met Police was forced to apologise in 2019 when the data sharing was revealed.

Greater Manchester Police used live facial recognition at the Trafford Centre, the UK's third-largest shopping centre, for six months in 2018 until an intervention from the then-Surveillance Camera Commissioner Tony Porter, who questioned the legal oversight of the scheme.¹⁹ Millions of people visit the centre every year and images were checked against a watchlist of missing people and "wanted" individuals – but Mr Porter expressed concerns about the proportionality of the use of LFR in the shopping centre.

In 2019, a Big Brother Watch investigation found several more instances facial recognition being used at privately owned sites in England. This included Meadowhall shopping centre in Sheffield, where the owners British Land told us that LFR was trialled for two days and then one month in early 2018. We estimate around 2 million people may have been scanned by LFR during the trial. Other sites were the Millennium Point, a mixed use development in Birmingham containing a conference centre, entertainment venues and educational institutions, and Liverpool's World Museum. Both were identified as

17 R(Bridges) v The Chief Constable of South Wales Police, Court of Appeal (Civil Division). EWCA Civ 1058, 11th August 2020, <https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf>

18 Facial Recognition Row: Police Gave King's Cross Owner Images Of Seven People, The Guardian, 4th October 2019, <https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people>

19 Greater Manchester Police Monitored Every Visitor To Trafford Centre For Six Months Using Controversial Technology Until They Were Told To Stop, Manchester Evening News, 14th October 2018, <https://www.manchestereveningnews.co.uk/news/greater-manchester-news/gmp-trafford-centre-camera-monitored-15278943>

police-linked LFR examples.²⁰ There was added irony in the World Museum using LFR at an exhibition of the Terracotta Warriors, on loan from China – the biggest user of facial recognition surveillance in the world.

All the police forces identified in our 2019 investigation had previously denied any involvement in LFR in our previous FOI requests to them. Following publication of our report, South Yorkshire Police admitted “supporting” a trial at Meadowhall,²¹ while the World Museum told us it used LFR on the advice of Merseyside Police and Millennium Point said it only operated LFR at the request of law enforcement, presumably West Midlands Police.²²

However, the police forces concerned did not admit to involvement in LFR, nor gave any further information in response to our subsequent FOI requests, and the venues concerned removed references to LFR from their privacy policies – Millennium Point even stated that it removed the information “at the request of law enforcement authorities”.²³ The investigation indicates that police forces may be secretly working with external and private sector organisations on covert uses of LFR on a scale totally hidden from public view.

On The Ground At Deployments

Big Brother Watch has staged demonstrations at the vast majority of Metropolitan Police LFR deployments over the past five years to observe the police’s behaviour, to offer support for those adversely affected and to show that Britain’s streets should not become biometric-powered police line-ups.

Signage Requirements

It is a requirement that the public is notified about the deployment of LFR around the specific location the technology is being used. The Metropolitan Police have also said they will publicise deployments in advance on social media. Often this has happened by the Metropolitan Police posting on Twitter a short time before a deployment begins. At the locations, there are sandwich board-style signs placed on busy streets to tell people what

20 Facial Recognition Epidemic In The UK, Big Brother Watch, 16th August 2019, <https://bigbrother-watch.org.uk/2019/08/facial-recognition-epidemic-in-the-uk/>

21 Freedom of Information Request from South Yorkshire Police to Big Brother Watch, ref. 20191992, 9 October 2019, <https://bigbrotherwatch.org.uk/wp-content/uploads/2020/01/South-Yorkshire-Police-private-company-facial-recognition-collaboration-October-2019redacted.pdf>

22 Facial Recognition Technology ‘An Epidemic In UK’, Says Big Brother Watch, Sky News, 16th August 2019, <https://news.sky.com/story/facial-recognition-technology-an-epidemic-in-uk-says-big-brother-wtch-11786567>

23 Millennium Point Privacy Notice, November 2022, <https://www.millenniumpoint.org.uk/wp-content/uploads/2022/07/CCTV-Privacy-Notice-V1.5.pdf> (accessed 26 April 2023)

is going on, but according to our observations, they are frequently missed. Big Brother Watch staff usually take placards to hold high in the air to raise awareness that facial recognition cameras are in use.



Often officers are handing out leaflets about the LFR deployment too but Big Brother Watch has observed that these officers are often well within the field of view of the cameras, and may even be next to the CCTV van – meaning the public have already been scanned before they can learn about what is going on.

The Right to Refuse

In general, the public has the right to opt out of having their face scanned by the police's live facial recognition cameras, and in theory, no negative inference should be drawn from an individual choosing to do this. Avoiding the LFR cameras alone is not justification for further police action.²⁴ However, Big Brother Watch has seen plain clothed police officers monitoring the edges of deployments in the past and questioning people who took alternative routes after seeing Big Brother Watch's placards or taking one of our leaflets – some of those officers have confirmed to us off record that they viewed such behaviour as justifying a police intervention. In Romford in 2019, a man was fined £90 for disorderly

²⁴ Standard Operating Procedure for Live Facial Recognition, Metropolitan Police, accessed 30th March 2023, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-sop.pdf>

behaviour after covering his face when passing the camera to object to the LFR scan, and allegedly swearing when physically apprehended by police.²⁵

Proving Innocence

Minutes from the Metropolitan Police's Facial Recognition Technology Strategic Board underline how LFR forces people to prove a negative, and how the police treat false matches.²⁶ In January 2022 the Met deployed LFR near Oxford Circus and one person triggered an alert who was subsequently stopped. They said they were not the person on the watchlist, that it was a false match, and provided ID to back this up. Despite having ID the minutes show that police wanted to subject the person to further biometric checks, using a mobile fingerprint scanner, and only accepted ID when this failed. It is worrying that the police were so willing to use further intrusive biometric checks, rather than accepting a clear ID document – and underlines how LFR matches place the onus on the individual to prove their innocence, even though an alert does not give police any additional powers.

Watchlists

A key part of deployments for police is creating the watchlist of people the LFR system is looking for in the crowd. The Metropolitan Police's watchlists for deployments since 2022 have ranged in size from around 5,800 people to almost 10,000 people.²⁷

Guidance from the College of Policing on Live Facial Recognition outlines who can be put on a watchlist, and it is not limited to fugitive criminals, including:²⁸

- a) Somebody wanted by the courts
- b) Someone suspected of an offence or where there are reasonable grounds to suspect that the individual is about to commit an offence
- c) Someone subject to bail conditions, a court order or restriction that would be breached if at the LFR camera site
- d) A missing person deemed to be at increased risk of harm
- e) Someone presenting as posing a risk of harm to themselves or others
- f) A victim of an offence

25 Moment Police Fine Pedestrian After He Covered Face From Facial Recognition Camera, Evening Standard, 16th May 2019, <https://www.standard.co.uk/news/london/moment-police-fine-pedestrian-after-he-covered-face-from-facial-recognition-camera-a4144156.html>

26 Minutes from the Facial Recognition Strategic Board from 9th February 2022, Freedom of Information Request to the Metropolitan Police, 01/FOI/21/023158, 7th May 2022

27 Metropolitan Police LFR Deployment Records, accessed 4th April 2023, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/lfr-deployment-grid.pdf>

28 Watchlist, Authorised Professional Practice: Live Facial Recognition, College of Policing, March 2022, <https://www.college.police.uk/app/live-facial-recognition/watchlist>

- g) A witness to an offence
- h) A close associate of someone in categories a) to e) above

At present the Metropolitan Police, which publishes the purposes for its LFR deployments, appears to have focussed on targeting criminal suspects and those wanted by the courts in its watchlist compositions.²⁹ However, Big Brother Watch observations have seen people on bail, who have no restrictions related to the area where LFR is being used, also being stopped following LFR alerts suggesting that either the watchlist compilation involves errors or the purposes for inclusion are wider than publicly stated.

The guidance states that watchlist inclusion should be based on an intelligence case, and reviewed from deployment to deployment. Officers are required to consider whether watchlist inclusion is excessive. Reference photographs must be lawfully obtained, with most sourced from custody image databases – which contain a significant number of unlawfully retained photos.³⁰ These images are police-originated where possible [primarily custody photographs] but non-police images [such as those taken from the internet] can be used at the discretion of the officer approving the LFR deployment.

According to the Metropolitan Police, the factors which feed into the intelligence case for including a person on the watchlist include:

- Offence severity
- Risk to the person, or the risk they pose to the public
- Crime trends, such as evidence of organisation or repetition
- Deployment location, which impacts who may pass through the LFR zone

In the deployment authorisation form for LFR use in July 2022 all details about the watchlist composition were redacted by the Met.³¹

Watchlist composition is also required to take heed of police forces' public sector equality duty [PSED], particularly regarding those aged under 18, 13 and those with a "relevant disability". Children generally have a greater expectation of privacy, while some people may have a disability which will undermine LFR accuracy. Guidance from the [then] Surveillance Camera Commissioner outlines in detail how police should construct watchlists with due consideration for the PSED.³²

29 Metropolitan Police LFR Deployment Records, accessed 4th April 2023, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/lfr-deployment-grid.pdf>

30 Authorised Professional Practice: Live Facial Recognition, College of Policing, May 2021, <https://assets.college.police.uk/s3fs-public/2021-05/live-facial-recognition-app.pdf>

31 LFR Application, Freedom of Information Request to the Metropolitan Police, FOI22/026317, 30th November 2022

32 Facing The Camera, Surveillance Camera Commissioner, November 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

The Met does not record the demographic breakdown of its watchlists - when asked for ethnicity breakdowns of its LFR alerts the force claimed providing this would be too costly.^{33,34} Anecdotally Big Brother Watch has observed that the vast majority of people stopped by the Met since 2020 following an LFR alert have been people of colour, mostly black people.

Bias in the watchlist itself is an often under-addressed part of the debate around LFR, as the tool will necessarily impact more on marginalised communities, if these people are more likely to be on a watchlist in the first place. Evidence around OIFR from South Wales, and nationally from fingerprint scanners, shows that black people were much more likely than their white peers to be subject to biometric surveillance, suggesting this may also be a concern with the compilation of LFR watchlist.³⁵

If the disproportionality in alerts were a consequence of disproportionality in the watchlists, even algorithmically flawless LFR could lead to certain groups being disproportionately flagged by the system and stopped in the street. Bias in watchlist construction is often forgotten in the discussion around LFR, but it is a major concern. The Met Police has internally acknowledged the risks of human bias in the system, and even called for research into this at a meeting in November 2021.³⁶ Unfortunately, its latest study focussed entirely on technological issues and did not address problems around human bias.

At least one watchlist was put together to target individuals deemed to be “fixated” on public figures, which was used alongside LFR at Remembrance Day 2017 in London.³⁷ The watchlist sourced data from the Fixated Threat Assessment Centre [FTAC], a joint police/healthcare unit set up “to assess and manage the risk to politicians, members of the British Royal Family, and other public figures from obsessive individuals”.³⁸ Some of the people on the list suffer from “serious mental illnesses and have fallen through the care net” according to the centre.³⁹

Police claimed it was “proportionate and necessary” to use a watchlist based on the Fixated Threat list to “identify persons whose precious [sic] behaviour at similar events has compromised the security plan”, or whose behaviour could “easily be expected to compromise the security in place” for the Remembrance Day service.⁴⁰

33 LFR Policy Document v.2, Metropolitan Police, accessed 5th April 2023, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document2.pdf>

34 Freedom of Information Request to the Metropolitan Police, FOI22/25956, 29th September 2022

35 #HandsOffOurBiodata: Mobilising Against Police Use of Biometric Fingerprint and Facial Recognition Technology, Stop the Scan [Racial Justice Network and Yorkshire Resists], October 2022, <https://stopthescan438237173.files.wordpress.com/2022/10/final-sts-20-22-foi-report-2.pdf>

36 FRT Strategic Board Meeting Minutes from 4th November 2021, Freedom of Information Request to the Metropolitan Police, 01/FOI/21/023158, 7th May 2022

37 Freedom of Information Request to the Metropolitan Police, FOI2018030000548, 15th March 2018

38 Fixated Threat Assessment Centre, Barnet, Enfield and Haringey Mental Health NHS Trust, accessed 4th April 2023, <https://www.beh-mht.nhs.uk/services/fixated-threat-assessment-centre-ftac/297>

39 Fixated Threat Assessment Centre, <http://www.fixatedthreat.com/ftac-welcome.php>, accessed 27th April 2023

40 Freedom of Information Request to the Metropolitan Police, FOI2018030000548, 15th March 2018

Images were either police custody images, or photographs captured by the police or FTAC outside a protected site, or at a previous event the individual attended.⁴¹

In a 2018 letter to the House of Commons Science and Technology Committee the then-Home Office minister Baroness Williams of Trafford claimed that watchlist at the Remembrance Sunday even was made up of people “forbidden from attending the event” or “wanted by the police”.⁴² However it was reported at the time that none of the 42 people on the list were wanted for a criminal offence.⁴³⁴⁴

The use of facial recognition in this non-criminal context led to an alleged “fixated” person being identified by the technology and subject to police action. Big Brother Watch was told this was either ejection, or close police supervision during the event. In post-deployment engagement with police Big Brother Watch was told that mental health groups had not been consulted, nor suitable advice sought from experts. There had also been no consideration of the potential psychological impact this intrusive surveillance may have had on vulnerable people.⁴⁵

Use Statistics

There have been 80 confirmed police deployments of overt live facial recognition in the UK, since Leicestershire Police first used it in June 2015 to scan the faces of the up to 90,000 people who attended that year’s edition of the rock and metal focussed Download Festival.⁴⁶ 21 of these deployments have been in London, 58 have been in South Wales [predominantly Cardiff and Swansea] and one was in Hull. It was estimated in submissions to the Court of Appeal relating to the Bridges case that South Wales Police had scanned around 500,000 faces.⁴⁷

Across those deployments there have been at least 3,315 matches [data is not available for all LFR uses], of which 340 are claimed to be true positives and the police admit 2,975 were false positives. This equates to 89.7 per cent of all matches obtained by UK police

41 Freedom of Information Request to the Metropolitan Police, FOI2018030000548, 15th March 2018

42 Letter from Baroness Williams to the Chair of the Science and Technology Committee, 28th March 2018, <https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf>

43 Police to use Facial Recognition Cameras At Cenotaph Service, The Guardian, 12th November 2017, <https://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph>

44 Freedom of Information Request to the Metropolitan Police, FOI2018030000004, 11th April 2018, https://www.whatdotheyknow.com/request/facial_recognition_used_on_the_r

45 Face Off: The Lawless Growth Of Facial Recognition In UK Policing, Big Brother Watch, May 2018, <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf>

46 The Police Are Scanning the Faces of Every Single Person at Download, VICE, 12th June 2015, <https://www.vice.com/en/article/64y37q/download-festival-is-a-police-trial-ground-for-facial-recognition>

47 R (Bridges) v Chief Constable of South Wales Police, EWCA Civ 1058, Court of appeal, 11th August 2020, <https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf>

using LFR overtly being false positives.⁴⁸

	Met Police	South Wales Police	Combined
True Positives	25	315	338
False Positives	150	2,825	2975
Total Matches	175	3,140	3313
True Positive per cent	13.3 per cent	10 per cent	10.2 per cent
False Positive per cent	85.7 per cent	90 per cent	89.8 per cent



86%
INNACURATE

Splitting the use statistics by force, the Met Police have had just 23 positive matches out of 173 total, meaning that 150 or 86.7 per cent were false positives, while South Wales Police have a false positive rate of 90 per cent [2,825 of 3,140 matches being incorrect]. Police seek to focus on the False Positive Identification Rate [FPIR], which is measured as the number of false positives as a proportion of the number of faces seen by the LFR cameras. This is often in the tens of thousands, with 2022 Met Police deployments detecting between 10,740 and 34,360 faces in just a few hours.⁴⁹ However, the police's way of measuring inaccuracy allows the number of errors to be concealed by the size of a crowd. For example, 100 false matches in a crowd of 10,000 could be presented as 99 per

⁴⁸ Stop Facial Recognition, Big Brother Watch, accessed 4th April 2023, <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>

⁴⁹ Metropolitan Police LFR Deployment Records, accessed 4th April 2023, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/lfr-deployment-grid.pdf>

cent accuracy or an error rate of 1 per cent, even though this is clearly a high number of mistakes to make.

An independent report commissioned by the Metropolitan Police and written by Professor Peter Fussey and Dr Daragh Murray at Essex University's Human Rights, Big Data and Technology Project, used the same methodology to Big Brother Watch in how it presented the proportion of true and false matches by LFR systems.⁵⁰ The most reasonable interpretation of operational accuracy must be the percentage of false alerts as a proportion of the total number of alerts, rather than as a measure against the number of people who passed the camera.

Data for the number of faces seen in deployments appears to only have been recorded consistently since 2020. In the eight functional deployments since then [one was cancelled due to faulty equipment] the Met Police estimates that 157,566 people's faces were biometrically scanned – with eight true positives and 24 false positives. This is a significant number of people who have been subjected to invasive scans to identify just eight people.⁵¹

Policy Analysis

Live facial recognition technology poses a significant threat to rights and freedoms in Britain and stands to fundamentally unbalance the relationship between police forces and citizens. Used widely in more authoritarian states like China and Russia, live facial recognition has no place in a purportedly rights-respecting, democratic nation.

Police use of LFR has continued to advance, despite growing public concern, a court ruling that found that South Wales Police's use of LFR was unlawful, a lack of Government strategy and no parliamentary consent. The technology has been deployed at shopping centres, festivals, sports events, concerts, community events – and even a peaceful demonstration. One force used the technology to keep innocent people with potential mental health issues away from a Remembrance Sunday event.

In our 2018 report *Face Off: The Lawless Growth of Facial Recognition in UK Policing*, we called on UK public authorities to immediately stop using automated facial recognition software.⁵² We also launched this call with support from parliamentarians, lawyers,

⁵⁰ Independent Report On The London Metropolitan Police Service's Trial Of Live Facial Recognition Technology, Professor Peter Fussey and Dr Daragh Murray, Human Rights, Big Data and Technology Project, University of Essex, July 2019, <https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf>

⁵¹ Legal Challenge: Ed Bridges v South Wales Police, Liberty, accessed 4th April 2023, <https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/#:~:text=The%20judgment%20means%20the%20police,were%20breached%20as%20a%20result.>

⁵² *Face Off: The Lawless Growth Of Facial Recognition In UK Policing*, Big Brother Watch, May 2018, <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf>

technologists and 25 human rights and racial justice groups.⁵³ The call was echoed by the only parliamentary committee to scrutinise live facial recognition, the Science and Technology Committee, which recommended an immediate moratorium on police use of LFR.⁵⁴ The Equality and Human Rights Commission made a similar recommendation, warning that facial recognition technology “may not comply with the UK’s obligation to respect privacy rights”.⁵⁵ Labour, the Liberal Democrats and the Green Party all pledged in their 2019 manifestos to regulate the use of facial recognition. Further, two London boroughs have passed symbolic motions in recent years to call for bans on facial recognition in their areas. Haringey Council voted in 2020 to support a motion demanding that the Metropolitan Police not deploy LFR in borough and calling on the force to halt the use of “any tactics which have a discriminatory impact”.⁵⁶ In early 2023, Newham Council also called for a moratorium on the technology in the east London area. The motion, which was passed unanimously, was proposed by Labour councillor for Canning Town North Areeq Chowdhury and called for a suspension of LFR in the borough at least until proper regulations around biometric surveillance anti-discrimination safeguards are implemented.⁵⁷ Five years on from our Face Off report, facial recognition poses perhaps an ever greater threat to our privacy and civil liberties, as technology further outpaces legislative scrutiny and democratic accountability.

LFR poses a risk both to individual privacy and to privacy as a social norm. The right to privacy is protected by the Human Rights Act 1998 and the European Convention on Human Rights. Human rights legislation requires that any interference with the right to privacy is in accordance with the law, necessary and proportionate. Police forces have failed to demonstrate that their use of live facial recognition meets this high bar.

LFR technology indiscriminately scans the faces of everyone who passes in front of the camera, with members of the public treated as potential suspects until a biometric identity check proves otherwise. In policing, suspicion has traditionally preceded surveillance and individuals are considered innocent until proven guilty. LFR reverses these important principles and in doing so normalises blanket, suspicionless surveillance. It cannot be considered proportionate. Police forces have also failed to make the case that LFR is strictly necessary and that other, less intrusive, means of locating and identifying suspects have not been pursued first.

53 Joint Statement On Police And Private Company Use Of Facial Recognition Surveillance In The UK, Big Brother Watch, September 2019, <https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019-1.pdf>

54 MPs call for halt to police’s use of live facial recognition, BBC News, 18th July 2019, <https://www.bbc.co.uk/news/technology-49030595>

55 Facial Recognition Technology And Predictive Policing Algorithms Out-Pacing The Law, Equality and Human Rights Commission, 13th March 2020, <https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law>

56 Haringey Says No To Facial Recognition Surveillance, London Post, 16th July 2020, <https://london-post.co.uk/haringey-says-no-to-facial-recognition-surveillance/>

57 Newham Council Rejects Use of Live Facial Recognition Technology, Computer Weekly, 19th January 2023, <https://www.computerweekly.com/news/252529364/Newham-Council-rejects-use-of-live-facial-recognition-tech-by-police>

The College of Policing's Live Facial Recognition Authorised Professional Practice [APP], published in March 2022, sets out guidance to police forces on their use of LFR.⁵⁸ The APP is extraordinarily permissive, setting virtually no limitations on police use of the technology. The APP sets out no criminal threshold for the use of LFR, claiming police can use LFR for non-crime events which fall under the nebulous category of causing "harm".

Of serious concern are the expansive categories of individuals that the APP suggests can be placed on a LFR watchlist. As well as those wanted for any category of criminal offence, watchlists can include a broad range of individuals, many of whom have committed no criminal offence and are not suspected of doing so.

Targeting "associates" of suspects, particularly of low grade crime, associates of those who might pose the "risk of harm", possible witnesses and even victims of crimes is an enormous expansion of policing surveillance. The sizes of the watchlists created for each deployment have already been steadily increasing. In November 2017, there were 42 people on the Met's watchlist; in January 2019 there were 2,401 people; and in July 2022 there were 6,858 people. [The APP] is likely to see the size of watchlists continue to increase. The Biometrics and Surveillance Camera Commissioner, Professor Fraser Sampson, has been critical of the guidance, stating that it "treats everyone like walk-on extras on a police film set rather than as individual citizens free to travel, meet and talk" and that this approach calls LFR's "legitimacy and proportionality into question".⁵⁹

For such a powerful and controversial technology, the lack of democratic mandate for the use of live facial recognition is deeply problematic. There is no legislation that directly addresses the use of LFR in public spaces, and the words 'facial recognition' do not appear in any laws in the UK. In our 2018 report, we warned:

"Automated facial recognition technology is currently used by UK police forces without a clear legal basis, oversight or governmental strategy, despite its potential to infringe on civil liberties and fundamental rights."

Police forces continue to rely on a patchwork of common law policing powers and out of date and inadequate legislation to justify the use of this technology. In *R (Bridges) v Chief Constable of South Wales Police & Information Commissioner*, a legal challenge to South Wales Police's use of live facial recognition at a Cardiff protest, the Court of Appeal found that LFR had not been deployed in accordance with the law. The College of Policing responded with the publication of new guidance (the APP) and commissioned the National Physical Laboratory to undertake a study into potential algorithmic bias in the technology.

⁵⁸ Live Facial Recognition Authorised Professional Practice, College of Policing, March 2022, accessed 3rd April 2023, <https://www.college.police.uk/app/live-facial-recognition>

⁵⁹ The Biometrics and Surveillance Camera Commissioner's response to the College of Policing APP on Live Facial Recognition - Biometrics and Surveillance Camera Commissioner, GOV.UK, 6th April 2022, <https://www.gov.uk/government/news/the-biometrics-and-surveillance-camera-commissioners-re-sponse-to-the-college-of-policing-app-on-live-facial-recognition>

In a statement to the House of Lords on LFR, Home Office Minister Baroness Williams of Trafford stated that due to *Bridges*: “we do not feel that there is any need for further legislation at this point.”⁶⁰ However, given the considerable rights impacts, we believe it is vital that political decisions must be made with regards to LFR to protect the public.

The use of LFR also has serious implications for the rights to free expression and assembly, which are also protected by the Human Rights Act and European Convention on Human Rights. We are concerned that the use of LFR has a “chilling effect” on people’s attendance of public spaces and events, harming their ability to express opinions and communicate with others in those spaces. As noted, LFR has already been deployed at an anti-arms fair demonstration in Cardiff, where the watchlist featured campaigners included for “intelligence” purposes, people not wanted by police at all.⁶¹ [The APP] also explicitly envisions LFR being used at “assemblies or demonstrations”, noting that the deployment of LFR could lead to people “feel[ing] less able to express their views or otherwise be more reluctant to be in the area”.⁶² The “chilling effect” of intrusive new forms of surveillance on freedom of expression has been well documented and recognised by the UN Special Rapporteur on The Rights to Freedom of Peaceful Assembly and of Association, the European Union Agency for Fundamental Rights and rights groups across the globe.⁶³

Anonymity is an important enabler of freedom of assembly and association, as assemblies traditionally have allowed participants a certain level of protection against being singled out or identified. In a 2020 report “Impact of new technologies” on the promotion and protection of human rights in the context of assemblies, including peaceful protests’, the UN High Commissioner for Human Rights stated that facial recognition has compounded this loss of anonymity that is critical to freedom of assembly and association:

“The rise of facial recognition technology has led to a paradigm shift in comparison with practices of audiovisual recordings, as it dramatically increases the capacity to identify all or many participants in an assembly in an automated fashion.

(...)

“The negative effects of the use of facial recognition technology on the right of peaceful assembly can be far-reaching (...) Many people feel discouraged from demonstrating in public places and freely expressing their views when they fear that they could be identified and suffer negative consequences.”⁶⁴

60 House of Lords Statement on Facial Recognition Surveillance, 27th January 2020, vol. 801, col. 1301

61 Big Brother Watch Correspondence with South Wales Police, 4th June 2018, <https://bigbrother-watch.org.uk/wp-content/uploads/2019/01/Arms-Fair-March-2018-additional-questions.pdf>

62 Live Facial Recognition Authorised Professional Practice, College of Policing, March 2022, accessed 3rd April 2023, <https://www.college.police.uk/app/live-facial-recognition>

63 Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, - Clément Nyaletsossi Voule, Special Rapporteur on the rights to freedom of peaceful assembly and of association, Human Rights Council, July 2019, A/HRC/41/41; <https://daccess-ods.un.org/tmp/9683250.78487396.html>

64 Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, UN Human Right Coun-

The considerable interference with freedom of expression that LFR poses cannot be justified.

The right to freedom from discrimination is also engaged by police forces' use of live facial recognition. Our analysis has found that police use of LFR is highly inaccurate. Since 2016, the Met's use of LFR has been 86 per cent inaccurate and South Wales Police has been 90 per cent inaccurate.⁶⁵ This appalling record demonstrates the ongoing risk of misidentifications. Surveillance technology with poor accuracy poses a risk to everyone, but is particularly disturbing in light of research showing that many facial recognition algorithms disproportionately misidentify black people and women.⁶⁶ In the context of law enforcement, biased facial recognition algorithms risk increasing the over-policing of ethnic minorities under the cloak of technological "objectivity".

The National Physical Laboratory's report into the NeoFace system used by the Met and South Wales Police demonstrates that the technology does have significant face and sex bias when used at certain settings.⁶⁷ The report concluded that police can mitigate these biases by adjusting the settings at which they operate the technology. However, police forces should not deploy technology associated with such serious bias. Furthermore, the make-up of watchlists also has the capacity to lead to discriminatory outcomes, if certain ethnicities or groups are disproportionately placed on watchlists.

The vast array of human rights issues posed by police use of LFR, coupled with the democratic deficit around its use mean it has no place in the UK.

RECOMMENDATION: The use of live facial recognition by police forces and private companies for public surveillance must be immediately stopped in the UK.

cil, 24th June 2020, A/HRC/44/24, <https://www.ohchr.org/en/documents/thematic-reports/ahrc4424-im-pact-new-technologies-promotion-and-protection-human-rights>

⁶⁵ These figures have been calculated from deployment statistics provided by the Metropolitan Police and South Wales Police. Since 2016, the Metropolitan Police has had 150 inaccurate matches and 25 correct matches. South Wales Police has had 2,825 inaccurate matches and 315 correct matches.

⁶⁶ Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use – Drew Harwell, the Washington Post, 19th December 2019, <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>

⁶⁷ Facial Recognition Technology in Law Enforcement: Equitability Study – National Physical Laboratory, NPL Report MS 43, Dr Tony Manfield, March 2023, https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf

“Because of how the technology works, facial recognition is more invasive than traditional CCTV surveillance – it’s more akin to having your fingerprints taken, and like many other people, I felt that was an invasion of my privacy”

- Dr Ed Bridges

Commentary From Dr Ed Bridges – Turning The Tide on Facial Recognition

“Back in 2017, when South Wales Police first started using facial recognition software on the streets of Cardiff, I was amongst the many thousands of innocent, law-abiding people who had their faces scanned and their biometric data taken. Because of how the technology works, facial recognition is more invasive than traditional CCTV surveillance – it’s more akin to having your fingerprints taken, and like many other people, I felt that was an invasion of my privacy. I had been doing nothing illegal, so why were my local police force intruding on my life?

“I was so outraged that I took the unusual steps of taking South Wales Police to court, to challenge why they were doing this. And after a lengthy legal battle, a landmark ruling by the Court of Appeal adjudged that South Wales Police’s use of automatic facial recognition technology had not been lawful. This represented a major step forward for civil liberties in the UK and reflects concerns that this technology is intrusive, authoritarian and discriminatory.

“One of the court’s key findings was that, because the technology involves capturing images and automatically processing sensitive personal data of many members of the public, most of whom won’t be of interest to the police, it is far more intrusive than traditional methods of surveillance. The Court found that there was not “the necessary quality of law” for it to be used within existing legislation or policies.

“The judgment also included a damning assessment of facial recognition’s inherent discriminatory nature. We know from multiple studies that facial recognition software struggles to recognise female and non-white faces, and yet the court judged that South Wales Police had “never sought to satisfy themselves... that the software program in this case does not have an unacceptable bias on grounds of race or sex”. The court also found that their Data Protection Impact Assessment failed properly to assess the risks to the rights and freedoms of members of the public who are scanned. At the time South Wales Police started using this technology, many of us felt their attitude towards human rights concerns was gung-ho and complacent; the judgment vindicated those concerns.

“Despite the judgment, many forces continue to use facial recognition software, despite it operating in a legal vacuum without adequate oversight or regulation. I am increasingly certain that this type of mass surveillance is anathema to anyone who wants to build a more equal and fairer society, not just because it treats everyone who might cross a camera’s gaze as a criminal, but because those unfortunate enough to be misidentified

are disproportionately likely to already be discriminated against in a host of other ways. We should be dismantling discrimination, not reinforcing it.”

Dr Ed Bridges is a civil rights campaigner from Cardiff

Retrospective Facial Recognition

Retrospective Facial Recognition [RFR] is the use of facial recognition software on either still images or video recordings taken in the past to compare faces to photographs held on police databases or watchlists.

Police in the United Kingdom broadly employ two forms of retrospective facial recognition; the first is “facial matching” on the central Police National Database which compares input images with the millions of custody images held by police, using a Cognitec algorithm.⁶⁸ The second is the set of more advanced retrospective facial recognition tools procured by individual police forces that are operated independently and rely on internal photograph databases. For this report, Retrospective Facial Recognition [RFR] will refer to the second form, while PND Facial Matching will refer to the first.

What is RFR?

RFR can be used in two ways: the “internal” use is where faces from probe images are compared with faces on the police database [such as mugshots] in an attempt to identify or match the probe image. The other use is “external” where a photo of a known person is compared to a set of images or videos in an attempt to identify them within the footage, often to track their location or movements. Currently, the former [internal] use is how UK police forces are deploying RFR.

Internal RFR is described by South Wales and Gwent Police as “a post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database in order to identify them.”^{69,70} Meanwhile, Cheshire Constabulary explains that RFR is used for “image identification” or asking “do we know this person?” and “recorded video identification – to I.D. people after an event/crime has taken place.”⁷¹ In London, documents supporting the Mayor’s Office for Policing and Crime to procure RFR say it will be used “to assist in identifying suspects from still images or specific images extracted from video.”⁷²

68 Use Of Facial Recognition Tech ‘dangerously Irresponsible’, BBC News, 13th May 2019

69 Facial Recognition Technology, South Wales Police, accessed 27th March 2023, <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/>;

70 Facial Recognition Technology, Gwent Police, accessed 27th March 2023, <https://www.gwent.police.uk/police-forces/gwent-police/areas/about-us/about-us/facial-recognition/>

71 Cheshire Police RFR Data Protection Impact Assessment, 7th September 2021

72 PCD 1008 Retrospective Facial Recognition System, MOPAC, 19th August 2021, london.gov.uk/sites/default/files/pcd_1008_retrospective_facial_recognition_system.pdf

Who Uses RFR?

Five UK police forces are currently using RFR, or are in the process of finalising their policy to implement it:

- South Wales Police
- Gwent Police
- Leicestershire Police
- Cheshire Police
- Metropolitan Police – who are finalising their RFR policy

All five of these forces use NeoFace, a facial matching tool from the Japanese company NEC. The same company also provides the Met Police's LFR software and in 2021 bought Northgate Public Services, a UK-based company which provided a host of software outsourcing for the public sector, including facial recognition.⁷³

According to documents on the Government's Digital Marketplace, a database of technology suppliers to the public sector, NEC NeoFace costs £40,000 per year, in addition to £1,500-£2,000 per 10,000 images enrolled in the database and up to £10,000 for the ability to process videos through the software. There are also a string of additional charges for onboarding, and optional extras including training and image quality assessment.⁷⁴

In London, the Mayor's Office for Policing and Crime [MOPAC] authorised a 4-year [2-year fixed term plus two single-year extensions], £3.1 million deal for the Metropolitan Police to buy RFR from Northgate Public Services in August 2021, suggesting that RFR has an annual cost to the Metropolitan Police in excess of £750,000.⁷⁵ This annual cost is similar to what would be expected if the Met Police enrolled all 3.5 million of its custody images at £2,000 per 10,000 [costing £700,000] in addition to the annual £40,000 cost and the £10,000 video processing package.

How is RFR Used?

NEC, whose NeoFace tool is currently dominant in the UK police market, claims that its product is capable of searching through databases made up of tens of millions of images

73 Northgate Public Services Becomes NEC Software Solutions, Bloomberg, 2nd July 2021. <https://www.bloomberg.com/press-releases/2021-07-02/northgate-public-services-becomes-nec-software-solutions>

74 NEC NeoFace G-Cloud Pricing Document, Government Digital Marketplace, accessed 27th March 2023, <https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-13/documents/92321/528277208343962-pricing-document-2022-05-17-0845.pdf>

75 PCD 1008 Retrospective Facial Recognition System, MOPAC, 19th August 2021, london.gov.uk/sites/default/files/pcd_1008_retrospective_facial_recognition_system.pdf

and that police forces can set up more than 100 image reference libraries.⁷⁶ On top of the facial recognition itself, the RFR packages are advertised as allowing police to then conduct a detailed comparison of facial images, create watchlists of still-unknown people's faces and use other information such as date of birth or "image tags" to filter results.

Cheshire Constabulary is the only force to currently have published substantial documents about its deployment of RFR, unlike South Wales Police and Gwent Police who are still to disclose significant detail, despite using the technology for a number of years. However, at the time of publication of this report, Cheshire Constabulary have since removed these documents from their website, raising concerns over transparency and accountability. When Cheshire Constabulary announced in June 2022 that it would introduce RFR, alongside OIFR, to help "identify offenders", the force's Assistant Chief Constable, Matt Welsted, claimed: "Facial recognition will not replace traditional means in identifying those who have committed a crime but adds to our arsenal and modernising the capability of our frontline".⁷⁷

According to the Data Protection Impact Assessment published by Cheshire Constabulary, probe images [photos of the unknown subject] can be taken from anywhere as long as officers establish the source of the photograph, so they can be sure there is a legal basis to use it before facial matching takes place.⁷⁸ Sources may include:

- CCTV
- Body-worn images are taken by officers when dealing with incidents or crime
- Social media
- E-fit images
- Other photos taken by officers on mobile phones/other devices
- Surveillance images
- Any other digital images, e.g. from dash-cams or doorbells

This illustrates the potential breadth of how police may employ RFR as the technology develops. Almost any image can be used for RFR identification – including computer-generated images as evidenced by the suggestion that an e-fit could be used in a facial search.

RFR is not used solely to find suspects, despite Cheshire Constabulary putting significant emphasis on identifying offenders in its public communications surrounding

⁷⁶ NEC NeoFace G-Cloud Service Definition Document. Government Digital Marketplace, accessed 27th March 2023, <https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-13/documents/92321/528277208343962-service-definition-document-2022-05-17-0845.pdf>

⁷⁷ Cheshire Police to roll out facial recognition technology, BBC News, 16th June 2022, <https://www.bbc.co.uk/news/uk-england-merseyside-61823941>

⁷⁸ Data Protection Impact Assessment (DPIA) (Retrospective FRT) – Cheshire Constabulary, accessed 15th August 2022, p. 4, <https://www.cheshire.police.uk/SysSiteAssets/media/downloads/cheshire/about-us/facial-recognition-technology/data-protection-impact-assessment-dpia-retrospective-frt.docx>

its rollout.⁷⁹

In its documents on RFR, the force admits that its facial matching tool could be used to identify:⁸⁰

- People deemed to be at risk or interacting with officers who are using their statutory powers
- Vulnerable people
- Victims of crime
- Anyone driving a vehicle
- Children
- People who are subject to police powers in the street*

**No detail is given on what this means but it may include people subject to stop and search.*

Far from being a “boost to victims of crime” as Cheshire Constabulary said when trumpeting its RFR rollout, RFR could be used to surveil victims of crime.

The force’s documents lay out the process for an RFR search of a facial image as follows:

1. An officer emails the probe image to the Visual Identification Unit [VIU].
 - a) All requests include details of the reason for the request and the provenance of the images being presented.
2. A search of Cheshire’s custody images, and West Coast Collaboration’s [North Wales, Merseyside and Cheshire] images, is then conducted via NeoFace technology.
 - a) The three forces hold around 1.36 million photos on their custody image database, with the potential to expand to other forces such as Dyfed-Powys
3. If no successful or conclusive match is obtained, the VIU will then try again using PND’s Face Search capacity.
4. Results of the matching process are returned to the officer in the case as intelligence, stating “Intelligence suggests that [image] may be [person]”.
 - a) NEC NeoFace scores matches between 0.000 and 1.000, with Cheshire Constabulary requiring a match score of 0.650 to be considered a “potential

79 Cheshire Constabulary To Roll Out Facial Recognition Technology To Help Identify Offenders And Take Them Off The Streets, Cheshire Constabulary, 16th June 2022, <https://www.cheshire.police.uk/news/cheshire/news/articles/2022/6/cheshire-constabulary-to-roll-out-facial-recognition-technology-to-help-identify-offenders-and-take-them-off-the-streets/>

80 Retrospective FRT Data Protection Impact Assessment (DPIA), Cheshire Constabulary, archived 27th October 2022, <https://www.cheshire.police.uk/SysSiteAssets/media/downloads/cheshire/about-us/facial-recognition-technology/data-protection-impact-assessment-dpia-retrospective-frt.docx>

positive” for officers to assess visually.⁸¹

5. If neither the NeoFace system nor PND search provides a suitable match result, the images will be uploaded to the database for future reference.

⁸¹ Facial Recognition Policy, Cheshire Constabulary, downloaded 23rd January 2023, since removed from the force's website

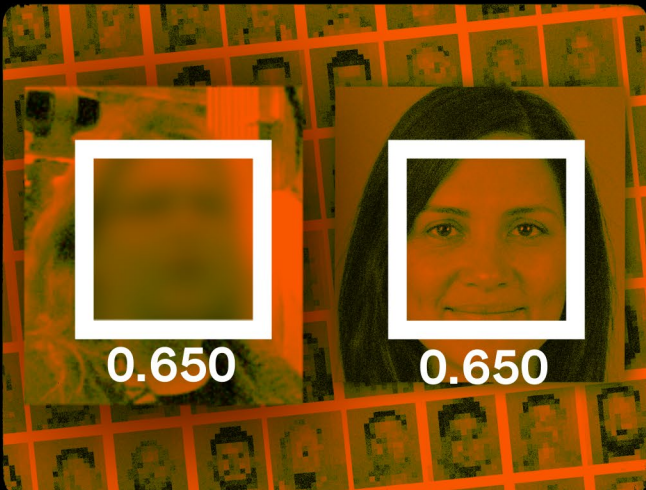
Officer emails probe image
to Visual Identification Unit



Search of custody
images conducted



Results of matching process
returned to the officer



If no suitable match,
images will be uploaded
for future reference



Operators in the police units conducting the RFR searches are sometimes given a significant number of potential matches to review, with South Wales Police presenting up to 200 possible hits to operators.⁸²

Police are currently supposed to use RFR as an intelligence tool and it is not deemed to meet the threshold to be treated as evidence. Officers are expected to “form their own mind” about the next steps to take; however Cheshire Constabulary does say that a RFR match could be sufficient grounds to arrest someone if other statutory requirements, such as the action being necessary, are met.⁸³

However, in practice, there are real concerns about whether RFR will invert the traditional standard of criminal proof that is someone is innocent until proven otherwise. In London, the former Deputy Commissioner, and Acting Commissioner, of the Metropolitan Police Sir Stephen House told the London Assembly Police and Crime Committee that: “the first thing we would do if someone is identified by [RFR], is we would interview them and say where were you at this time and place, and if they have an alibi that stands up, then clearly there’s a problem with the facial recognition”.⁸⁴

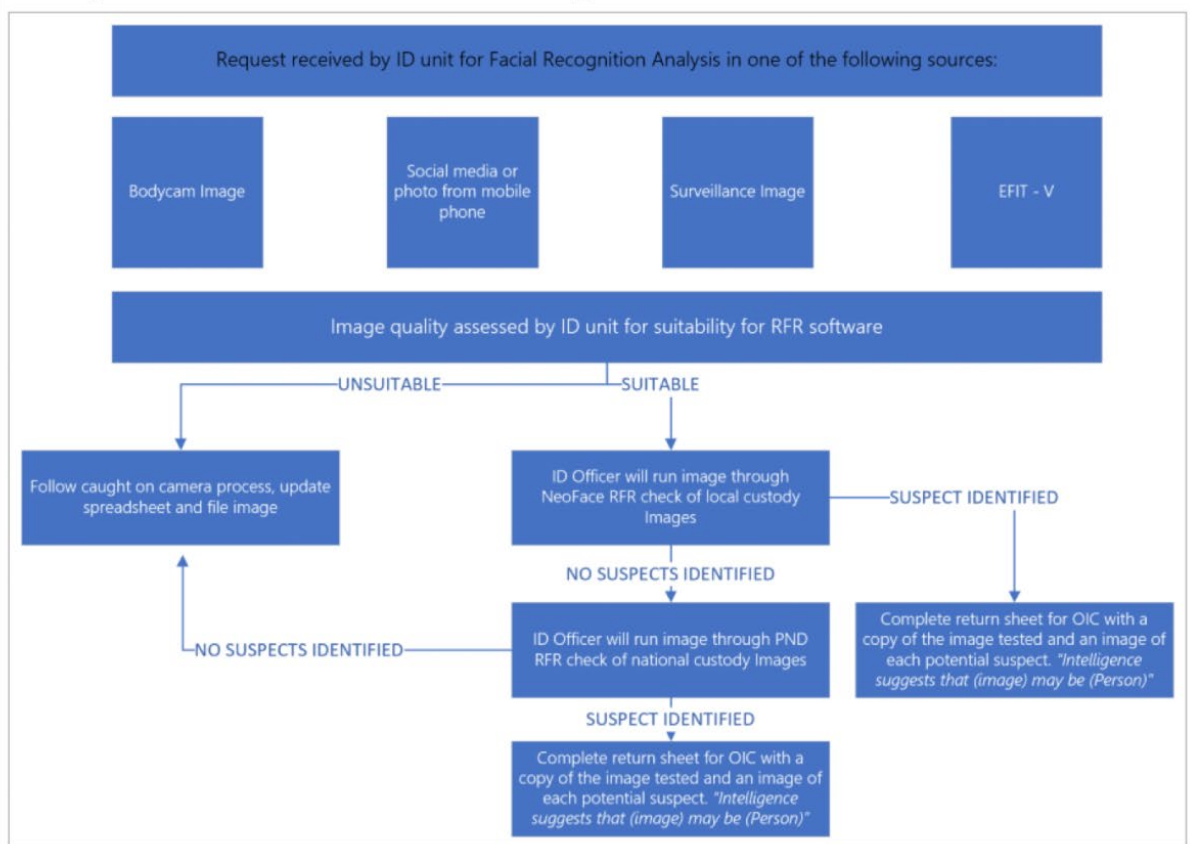
This statement implies that a match will put the onus on an individual to prove they are not who the technology suggests they could be in the Metropolitan Police’s jurisdiction. A false positive could lead to somebody being asked to attend a police station for an interview for no reason bar algorithmic error. It is also difficult to prove a negative, and innocent people could have difficulty if they are not the person in a blurry image contrary to a computer’s suggestion.

82 Facial Recognition Technology, South Wales Police, accessed 25th March 2023, <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/>

83 Retrospective FRT Data Protection Impact Assessment (DPIA), Cheshire Constabulary, downloaded 23rd January 2023, since removed from the force’s website

84 Live And Retrospective Facial Recognition Technology, Caroline Russell, YouTube, 22nd December 2021, https://www.youtube.com/watch?v=bGv5_OCz4h0

Example Information Flow for RFR images identification:



Statistics

Of the forces presently using RFR only three have provided data on how frequently they use the technology, whilst the Met has not finalised its rollout and Leicestershire Police failed to respond:

- Cheshire Police used RFR 1,935 times between 14th October 2021 and 18th December 2022, which equated to an average of 4.5 uses a day or just over 126 uses per month.⁸⁵
- South Wales Police said it used RFR 4,849 times in the 12 months to 16th December 2022, i.e. 13.3 times a day or 93 times a week.⁸⁶
- Gwent Police used RFR 689 times in the year to 16th December 2022, i.e. just under twice a day and just more than 53 times per month.⁸⁷

⁸⁵ Freedom of Information Request to Cheshire Constabulary 15732, 9th January 2023

⁸⁶ Freedom of Information Request to South Wales Police 1236/22, 17th January 2023

⁸⁷ Freedom of Information Request to Gwent Police 25731, 9th January 2023

In a June 2022 update published online, South Wales Police claimed to have achieved nearly “4,000 possible matches”, with an average of 100 every month.⁸⁸ This was a sharp increase on the claim made in 2018 by a SWP spokesperson of “over 2,000 positive matches” leading to “over 450 arrests”.⁸⁹ The 2018 claim implies that around 22.5 per cent of positive matches led to an arrest, and applying this statistic to the more recent match data implies that from the 4,000 “possible matches” to June 2022, there may have been fewer than 1,000 arrests.

With only one in four positive matches leading to an arrest, the figures already suggest that SWP are making relatively few arrests as a result of RFR. When figures around the total number of RFR searches, including those not leading to a potential match, are analysed the utility of the technology becomes even less clear.

Another SWP report from 2018, which can no longer be found at its original web link but is available on internet archives, said only 22 per cent of RFR searches led to matches that were actively confirmed by SWP officers, or around one match for every five searches.⁹⁰

Applying these two figures to the number of RFR searches actually conducted in South Wales, the 4,849 uses by force would yield 1,067 positive matches [22 per cent match rate on searches], leading to 240 arrests [22.5 per cent of positive matches resulting in arrest]. An estimated figure of 240 arrests from 4,849 RFR searches implies that only around five per cent of all searches end up with someone being arrested – a much smaller proportion than the numbers cited by SWP spokespeople.

Although there may have been some algorithmic improvements, and improvements in the procedures around probe image protocol since the 2018 report, these numbers suggest that RFR does not yield a significant number of arrests. It is not clear how many of those arrested could have been identified by other means in any case.

88 Is There A Legitimate Role For Facial Recognition In Policing And Law Enforcement?, South Wales Police, 29th June 2022, <https://www.south-wales.police.uk/news/south-wales/news/2022/meh-jun/facial-recognition-technology-testimony/>

89 South Wales Police Defend Facial Recognition Software Amid Criticism Over Inaccurate Matches, The Huffington Post, 5th May 2018, https://www.huffingtonpost.co.uk/entry/south-wales-police-defend_uk_5aed6d33e4b0c4f19322d1ff

90 An Evaluation Of South Wales Police’s Use Of Automated Facial Recognition, Bethan Davies, Martin Innes & Andrew Dawson, Crime & Security Research Institute, Cardiff University, September 2018

Police National Database Face Search

All UK police forces have access to a form of RFR via the police national database [PND], with the Face Search capability being introduced in 2013.⁹¹

What Is the PND?

The PND is a nationwide system that acts as a data repository of a huge quantity of police photos, information and intelligence which is uploaded by individual forces. This includes information on events, organisations and people.⁹² Police are given the power to take photographs of people when they are held after being arrested under Section 64A of the Police and Criminal Evidence Act 1984.⁹³ Police forces can upload these custody images from their own systems to the PND. It is these custody images which make up the majority of the reference database for the PND Face Search tool.

How Does Facial Searching Work?

Recent documents outlining the PND Facial Searching process have not been published, with most police forces citing exemptions around law enforcement or national security when asked for a copy of up-to-date guides via Freedom of Information Requests. However, a redacted 2014 copy of PND Facial Searching guidance has previously been disclosed and provides some insight, although this may have been updated since.

Images were given a maximum file size of just 500KB, which is a fraction of the file size of a photo taken on a flagship smartphone released in 2014 underlining the small size of images used for PND searching.⁹⁴ Photos can be any image of a face, from custody images to CCTV screen grabs. Information about the criteria for searching is redacted under Section 31 of the Freedom of Information Act [the law enforcement exemption]– but the document states that searches will return either a failed or saved result, with the latter being a successful search. Searches occur by comparing the probe image against the millions of images on the PND and returning matches that are above the similarity

91 Dr Eilidh Noyes (University of Huddersfield) and Dr Reuben Moreton (Reli Ltd) Written Evidence on New Technologies and the Application Of The Law, NTL0026, Justice and Home Affairs Committee of the House of Lords, 21st October 2021, <https://committees.parliament.uk/writtenevidence/38730/pdf/>

92 Police National Database [PND] Procedure, North Yorkshire Police, Fire and Crime Commissioner, accessed 29th March 2023, <https://www.northyorkshire.police.uk/SysSiteAssets/foi-media/north-yorkshire-police/our-policies-and-procedures/criminal-justice/police-national-database-procedure2.pdf>

93 Section 64A, Part V, Police and Criminal Evidence Act, 1964, <https://www.legislation.gov.uk/ukpga/1984/60/section/64A>

94 Facial Recognition Search on The Police National Database, Home Office, 2014

threshold.

In 2017, 12,504 facial searches were conducted on the PND, a sharp rise from 3,360 in 2015. However, Home Office research found that the face matching algorithm performed at a significantly worse standard than a human being, finding 20 matches from 211 searches in a test – whereas a person identified 56 matches from the same set of images.⁹⁵

How Many Images Are On It?

As of January 2023, there are 16,102,341 images held on the Police National Database.⁹⁶ This is a decrease of around three million from five years ago. However, the 2023 figure comes after the deletion of almost six million images as part of a system upgrade in 2021, many of which were low quality or duplicates.^{97,98} A huge number of new images are being added to the PND every year according to data from the Home Office, with 1.9 million being added in 2020, 1.1 million in 2021 and 982,000 in 2022 – totalling around four million extra photos in three years. Over the three years this equates to around 3,600 photos being added a day, or 2.5 per minute. Multiple images may be held of the same person, and whilst most photos are of faces, some may be of other identifiers such as tattoos and scars.

When Big Brother Watch's first Face Off report was published in 2018, 12.5 million of the 19 million images on the PND were deemed of a quality that was biometrically searchable with facial recognition.⁹⁹ In 2023, the Home Office refused to disclose updated figures claiming that it would harm national security.¹⁰⁰ However, given that 5.8 million low-quality images were deleted in a 2021 update to the Facial Search system it is reasonable to assume that the proportion of the 16.1 million images on the PND that are enrolled in facial recognition is even higher than the 66 per cent figure from 2018.

Unlawful Retention of Custody Images

One does not have to have ever been convicted of, or even charged with, an offence to feature on the PND. As custody images are taken on arrest there are likely millions of

95 Use Of Facial Recognition Tech 'dangerously Irresponsible', BBC News, 13th May 2019, <https://www.bbc.co.uk/news/technology-48222017>

96 Freedom of Information Request to the Home Office, FOI74340, 1st March 2023

97 Face Off, Big Brother Watch, May 2018, <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf>

98 Freedom of Information Request to the Home Office, FOI74340, 1st March 2023

99 Oral Evidence – Biometrics Strategy and Forensic Services, Science and Technology Committee of the House of Commons, HC 800, 6th February 2018, <https://committees.parliament.uk/oralevidence/7582/pdf/>

100 Freedom of Information Request to the Home Office, FOI75104, 30th March 2023

innocent people whose photos may have been uploaded and retained in the PND by a police force, without their knowledge and justification.

More than a decade ago, in 2012, the High Court ruled in a case known as “RMC” that the Metropolitan Police’s retention and storage of custody images taken from people who were not convicted of a crime was unlawful and breached human rights legislation.¹⁰¹ Following this ruling the Home Office commissioned the 2017 Custody Image Review which laid out the criteria for deleting custody images following requests from the public. A subsequent review was due to take place in 2020, but this has not happened.¹⁰² A key recommendation from the review was that when police forces receive a request to delete custody images, there should be presumptions either in favour or against deletion based on whether someone was convicted, the severity of their offence and their age on arrest/conviction.

Big Brother Watch asked every police force in the country what information they provide to arrestees about their data rights concerning their custody images, particularly if they are not charged or convicted. The vast majority do not provide specific information about this right, often referring to a Home Office notice on entitlements for people in police detention published in 2018, which does not make people aware of this right. It is alarming that a decade after the RMC ruling most police forces are not making people aware of their data rights and are continuing to retain images unlawfully.

Despite many police forces in England and Wales, including those that use facial recognition outside of the PND, claiming that there are technical challenges in removing innocent people’s photos from their custody databases, the challenge is not insurmountable. Police Scotland has a system set up to automatically delete photos of non-convicted people from its database.¹⁰³ It can do this as the computer systems in the Scottish court service are connected to Police Scotland, but this is not the case in the rest of the UK. Clearly, this suggests that setting up a system or committing staffing resources to remove innocents’ images is possible, however, it appears to not be a priority – despite the huge sums spent by police forces on facial recognition technology.

Professor Paul Wiles, who was the Biometrics Commissioner in 2017, warned that hundreds of thousands of innocent people’s custody images were held on the database but this figure is an estimate.¹⁰⁴ Six years on, the Home Office still does not know how many

101 RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department, EWHC 1681 [Admin], 2012, <https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf>

102 Custody Image Review, Home Office, February 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf

103 The Police National Database (PND), Geoff White, 13th May 2019. <https://geoffwhite.tech/2019/05/13/the-police-national-database-pnd/>

104 Facial Recognition Database ‘Risks Targeting Innocent People’, BBC News, 14th September 2017, <https://www.bbc.co.uk/news/uk-england-tyne-65128383>

innocent people's photographs are held on the PND.¹⁰⁵

Professor Fraser Sampson, who took over as Biometrics and Surveillance Camera Commissioner in 2021, wrote in his 2020 Annual Report that few forces were actively working to delete innocent people's images and instead continue "to retain the vast majority of their custody images indefinitely, regardless of whether the individual has been convicted of an offence".¹⁰⁶ He also expressed concern about the incredibly slow pace of proposed technical solutions to hasten and automate the deletion of unlawfully held photographs.

Big Brother Watch asked all 45 territorial police forces in the UK how many requests for deletion they had received from 2020 to 2022. 24 of the 45 gave numbers in response to Freedom of Information Request, adding up to 2,784 requests over the three years, of which 1,523 were agreed to by police. A small number of people who made requests did not have a photo on the system which is included in the non-approved requests. More than half the requests were made to the Metropolitan Police alone while some forces refused or were unable to give any stats.¹⁰⁷

Extrapolating the number of requests to estimate the statistics for the entire country, the 2,784 figure would equate to around 5,220 deletion requests nationally if all police forces provided data. 5,220 deletion requests in three years equates to just one person getting their photo erased for every 665 added to the system over the same period.

It is therefore obvious that a significant number of innocent people's custody images are being uploaded and retained in the PND each year – despite the High Court ruling the retention policy to be unlawful and a breach of individuals' right to privacy. Unless the conviction rate for people arrested is more than 99.9 per cent, there is clearly a greater number of innocent people arrested and photographed annually than innocent people's photos being deleted.

Despite the poor level of accuracy with the PND's facial searching algorithm the sheer number of images, lawfully and unlawfully held on it, underline its potential to transform into a mass-facial recognition search engine for the police. The Home Office is now funding a new biometrics search program, including facial recognition, which vows to give law enforcement in the UK the ability to search faces with much greater accuracy than the PND allows.

105 Freedom of Information Request to the Home Office, FOI74340, 1st March 2023

106 Biometrics Commissioner Annual Report 2020, November 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1036487/E02669527_Biometrics_Commissioner_ARA_2020_Text_Elay.pdf

107 South Yorkshire Police additionally provided said it received 162 requests for deletion but was unable to give figures for the number of these that led to being deleted.

Policy Analysis

Police forces have been using RFR with limited success for a number of years, matching images and videos of suspects against custody images held in the PND. RFR poses different rights concerns to live facial recognition, as it is not a live surveillance tool used on the public at large. However, without strong legal safeguards, RFR could grant police forces enormous power to identify and track individuals through time and across different locations.

Risk to privacy

The ability of police forces to biometrically process and potentially identify anyone that they hold facial images of [through either photographs or videos] is a serious risk to our privacy and our ability to move through public space with anonymity. The processing of sensitive, personal biometric data must be strictly regulated in order to be compliant with human rights law.

Police forces have relied on the argument that petty criminals can escalate to more serious offences in order to justify the broad use of RFR for a wide range of offences including very “low-level” crime. Cheshire’s DPIA claims that people who “start by committing low level crime i.e. theft from washing lines, can move on to commit further and more serious crimes, if not identified and dealt with”.¹⁰⁸ A reliance on hypothetical future serious offences as a justification for using biometric surveillance for very “low level” crimes is an inappropriate way in which to assess necessity and proportionality, and would mean that almost any use of RFR could be deemed as legitimate. This concerning approach to RFR underlines the potential for the technology to become a tool for even greater mass monitoring.

Currently, the lack of safeguards and the almost entirely unfettered use of this technology means it cannot be considered necessary or proportionate. Police forces have not made the case that the use of RFR is strictly necessary, nor do they propose restricting its use to cases where other less invasive methods of identifying suspects have been exhausted. Before RFR is used, forces must publicly set out why this technology is necessary.

As noted, RFR is being used for virtually any policing need, absent of even a criminal threshold. Given the intrusive nature of RFR, a threshold should be introduced limiting the use of RFR only where strictly necessary in relation to an individual suspected of committing a qualifying offence. Qualifying offences are sexual, violent, terrorism and burglary offences and are outlined in Section 65A of the Police and Criminal Evidence Act 1984. Qualifying offences are also used as a threshold in policies governing police

¹⁰⁸ Retrospective FRT Data Protection Impact Assessment (DPIA), Cheshire Constabulary, downloaded 23rd January 2023, since removed from the force’s website

retention of fingerprint and DNA data.

RECOMMENDATION: In recognition of the intrusive nature of retrospective facial recognition, police should have limitations on the circumstances in which it can be used. A biometric search should only be undertaken when strictly necessary to identify an individual suspected of carrying out a qualifying offence, as defined by Section 65A of the Police and Criminal Evidence Act 1984.

Lack of legal basis

The legal framework police forces are currently relying on to justify their use of RFR is woefully out of date and provides only minimal safeguards. The Ryder Review, an independent review of the governance of biometric data in the UK, stated:

“The governance of biometric data at present relies on a patchwork of overlapping laws addressing data protection, human rights, discrimination and criminal justice issues. There is no single overarching legal framework for the management of biometric data. Sources of law that developed in response to more general issues cater for the management and regulation of biometric data in an ad hoc manner.”¹⁰⁹

The Home Office admitted in its 2018 Biometrics Strategy that “policing in England and Wales does not have common standards for the capture, storage or exchange of facial image data.”¹¹⁰ Cheshire Constabulary is the only force to provide detailed information about their use of RFR, although these documents have now been removed from their website. The force stated that the following pieces of legislation provide the legal frameworks that apply to their use of RFR:

- Police and Criminal Evidence Act 1984
- Criminal Procedure and Investigations Act 1996
- Data Protection Act 2018¹¹¹

The police derive their powers to obtain an individual’s image from Section 64A of the Police and Criminal Evidence Act 1984 [PACE]. It is under these powers that police forces obtain probe images and images that make up image reference libraries. Cheshire Constabulary have stated that under data protection law, the relevant lawful basis for the processing of

109 The Ryder Review: Independent legal review of the governance of biometric data in England and Wales – Matthew Ryder, Ada Lovelace Institute, June 2022, p. 21, <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf>

110 Biometrics Strategy – Home Office, June 2018, pg. 18, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf

111 Data Protection Impact Assessment (DPIA) (Retrospective FRT) – Cheshire Constabulary, accessed 15th August 2022, <https://www.cheshire.police.uk/SysSiteAssets/media/downloads/cheshire/about-us/facial-recognition-technology/data-protection-impact-assessment-dpia-retrospective-frt.docx>

these custody images via RFR is Section 35(2)(b): “The processing is necessary for a task carried out for a law enforcement purpose by a competent authority.”¹¹² This “task” [RFR] is justified by the Criminal Procedure & Investigations Act 1996 Code of Practice [section 3.5]: “In conducting an investigation, the investigator should pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances.” This does not, however, grant police forces a blank cheque for pursuing any line of inquiry, by any method. Article 8 of the Human Rights Act requires intrusions into privacy be both necessary and proportionate, which at present, police force use of RFR cannot be said to be.

The Police and Criminal Evidence Act 1984, the Criminal Procedure and Investigations Act 1996 and the Data Protection Act 2018 do not address automated facial recognition, let alone RFR, in any direct or substantial way. This paucity of binding regulation paves the way for misuse of the technology. The Government’s failure to regulate RFR is a failure to safeguard protected rights to privacy, freedom of expression and freedom of assembly and means authorities’ uses of the technology may not be in accordance with the law.

RECOMMENDATION: There is currently no evidence base, nor a clear and sufficient legal framework, for the use of RFR. If police make a strong business case for the strict necessity of RFR, the Government should consider it and, before any operational use of RFR, introduce new primary legislation in order to bring in the safeguards and restrictions on the use of RFR as outlined in the recommendations in this report.

Police collection and processing of facial images, to be used as probe images or to create image reference libraries, has the potential to significantly expand the scope of RFR. In the US, it is estimated that images of one in two US adults are in facial recognition databases used to identify criminal suspects.¹¹³ Police forces are able to search not only regional and state databases, but also FBI criminal and civil databases [Next Generation Identification]. The FBI has stated it needs “to collect as much biometric data as possible... and to make this information accessible to all levels of law enforcement, including International agencies.”¹¹⁴ This level of data collection for RFR purposes is not currently [publicly] envisioned in the UK, but it should act as a warning to UK policymakers as to the vast potential scope of RFR if left unregulated.

The PND’s “Face Search” and police RFR systems use images which ought to have been deleted from police systems, incurring not only a privacy intrusion through the unlawful

112 Data Protection Impact Assessment (DPIA) (Retrospective FRT) – Cheshire Constabulary, accessed 15th August 2022, <https://www.cheshire.police.uk/SysSiteAssets/media/downloads/cheshire/about-us/facial-recognition-technology/data-protection-impact-assessment-dpia-retrospective-frt.docx>

113 The Perpetual Line-Up: Unregulated Police Face Recognition in America, The Georgetown Law Center on Privacy and Technology, 18th October 2016, accessed 9th January 2023, <https://www.perpetuallineup.org/>

114 Testimony of Jennifer Lynch to the Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law, Electronic Frontier Foundation, 18th July 2012, https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf

retention and biometric processing of such images, but risking serious consequences for innocent individuals who could be wrongly flagged as suspects, witnesses, victims or associates of those.

Cheshire Constabulary also admits there is the potential for unlawfully retained images to be used in RFR as it, like all forces, holds a large number of photographs of innocent people that should have been deleted. There is further detail on the unlawful retention of custody photos in the section of this report on PND Facial Matching, and those concerns apply equally to RFR.¹¹⁵

In order for the use of RFR by police forces to have the possibility of being considered proportionate, the custody images of unconvicted people must be deleted from police image reference databases. After years of inaction, the Home Office and police forces must ensure that the deletion of unconvicted individuals from both the PND and police force's own databases is prioritised.

RECOMMENDATION: The Home Office must work with police forces to ensure the automatic deletion of the thousands of images of unconvicted individuals from the Police National Database and police force databases. Police forces should only be permitted to carry out retrospective facial recognition searches on lawfully held custody images.

As outlined, police forces collect probe images from a wide range of sources, including CCTV, body cam footage, video doorbells and social media. It could be reasonable for lawfully held police originated images, such as custody images, police body cam footage taken in a lawful and proportionate way and photos taken lawfully during policing operations, to be used for RFR purposes, provided these purposes are strictly regulated, meet a high threshold of strict necessity, and only apply to crimes of a higher severity.

When police forces collect and retain non-police originated images, such as CCTV footage or social media images, for the purpose of RFR searches, there should be additional consideration of the privacy intrusion. Compliant police originated images should be preferred for use as probe images, as individuals will have the lowest expectations of privacy. Images from non-police or non-compliant sources should be used only when other options have been exhausted.

RECOMMENDATION: Police forces must respect the privacy rights of individuals when sourcing probe images. Probe images from non-police originated sources should be collected and processed only where police originated images are unavailable.

¹¹⁵ Retrospective FRT Data Protection Impact Assessment (DPIA), Cheshire Constabulary, downloaded 23rd January 2023, since removed from the force's website

Home Office Biometrics Programme

With several police forces procuring their own retrospective facial recognition technology and the PND Facial Search's known flaws, the Home Office is currently in the process of securing a supplier for a nationwide face-matching database as part of its wider Biometrics programme.

The Home Office Biometrics [HOB] Matcher, sometimes called the Strategic Matcher, is being designed as a technology platform and a service to offer biometric search, identification and verification across fingerprints and facial scans.¹¹⁶ Initially, the system will focus on fingerprint matching for law enforcement but the goal is to use the HOB Matcher for immigration and law enforcement across both biometrics.

Several multi-million pound contracts have been awarded in relation to the HOB programme since it began in 2017, including:

- £28,000,000 to Fujitsu for five years of core IT services underpinning the project from 2018;¹¹⁷
- £49,800,000 to an unknown company in a contract beginning in June 2023 for services to support the matcher platform.¹¹⁸

At present, two separate fingerprint databases are used for comparison and matching across the UK: IDENT1 which covers law enforcement and security, and IABS which covers immigration and citizenship. These are in the process of being combined into a "mega-database"¹¹⁹ albeit logically separated with role-based access controls in an attempt to ensure data and activities are only accessible to individuals with the relevant permissions.¹²⁰

Although there is little information currently in the public domain about the Home Office's development of facial recognition as part of the HOB, some police forces do see this national system as a viable alternative to procuring their own RFR systems. Avon and

116 Home Office Biometrics Programme Briefing Paper, Home Office, 17th July 2019, https://privacyinternational.org/sites/default/files/2020-08/OP1071%20-%2017072019%20Item%208.1%20LEDSHOB%20Open%20Space%20-%20HOB%20Programme%20Briefing_0.pdf

117 Home Office Biometrics Biometric Matcher Platform and Associated Services – Lot 1, Contracts Finder, 27th February 2018, <https://www.contractsfinder.service.gov.uk/notice/21319a82-4a57-4b62-8eff-57a320a2328e?origin=SearchResults&p=1>

118 Biometric Matcher Platform and Associated Services, Contracts Finder, 1st April 2022, <https://www.contractsfinder.service.gov.uk/notice/f536ae4e-25a6-411a-b054-19ddca7e2213?origin=SearchResults&p=1>

119 Home Office Biometrics Programme Briefing Paper, Home Office, 17th July 2019, https://privacyinternational.org/sites/default/files/2020-08/OP1071%20-%2017072019%20Item%208.1%20LEDSHOB%20Open%20Space%20-%20HOB%20Programme%20Briefing_0.pdf

120 Strategic Matcher Phase 1A Privacy Impact Assessment, Home Office, 1st August 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721101/Strategic_Matcher_Phase_1a_PIA_Final_.pdf

Somerset Police said it had paused efforts to obtain its own RFR tool as it has a potential opportunity to match up with the national strategic matcher programme.¹²¹

However, it is reasonable to assume that as fingerprint databases are being amalgamated to create a single “mega-database” this is a likely scenario too for facial images. The Home Office is already ultimately responsible for the PND, which contains more than 16 million photographs. It also controls several immigration databases that contain facial images of millions more people.

A February 2023 assessment of the HOB clarified that police and counter-terrorism units already have access to facial searching of immigration databases – potentially putting a huge number of innocent people in the scope of facial recognition searches.¹²² Later phases of the ongoing HOB will integrate further immigration databases, while the final state is the real-world deployment of facial matching for law enforcement.¹²³

Big Brother Watch was unable to obtain any documents about the tender outlining use of facial matching in the HOB because the contract award process was an ongoing exercise at the time of publication of this report and the DPIA is yet to be published.¹²⁴ This means it is unclear how the database will be constructed to ensure logical separation between datasets so that people are not subject to unjustifiable facial searches. The blurring of the lines by some police forces when conducting mobile fingerprint scans, as outlined in the discussion on OIFR further in this report, has the potential to cause harm. The lawfulness of retaining and using images of innocent people for facial searching as in *R (RMC and FJ) v Metropolitan Police Commissioner* must also be considered.

Broadly, the concerns about a centralised RFR database are similar to those about how individual forces use RFR, with the additional risks posed by the centralising databases across many uses only exacerbating these concerns.

121 Freedom of Information Request to Avon and Somerset Police, FOI1233-22, 30th November 2023

122 Accounting Officer Assessment: Home Office Biometrics (HOB) Programme, Home Office, 24th February 2023, <https://www.gov.uk/government/publications/home-office-major-programmes-accounting-officer-assessments/accounting-officer-assessment-home-office-biometrics-hob-programme>

123 Biometric Matcher Platform and Associated Services, Contracts Finder, 1st April 2022, <https://www.contractsfinder.service.gov.uk/notice/f536ae4e-25a6-411a-b054-19ddca7e2213?origin=SearchResults&p=1>

124 Freedom of Information Request to the Home Office, FOI74080, 15th February 2023

Operator Initiated Facial Recognition

Operator Initiated Facial Recognition [OIFR] is the deployment of facial recognition technology via a mobile phone, making use of a dedicated app alongside the device's camera. It is a street policing tool, similar to mobile fingerprint scanners, as it requires relatively basic equipment compared to Live Facial Recognition.

Who Uses OIFR?

Three UK police forces have used the technology: South Wales, Gwent and Cheshire. The two Welsh forces ran a trial of OIFR from December 2021 until March 2022 while Cheshire appears to be in the process of rolling out the technology.^{125,126} The outcome of the Welsh trial in relation to future use it still pending.

How is OIFR Used?

According to police forces, OIFR is used to attempt to identify people in a number of different situations, including those who are wanted for criminal offences and those deemed to be posing a risk of harm to themselves or others.¹²⁷ South Wales and Gwent Police's joint documents [referred to hereafter as the South Wales Police documents] published concerning its trial claim that OIFR is a "valuable" tool that helps officers fulfil their common law policing duties. Examples of potential use cases include:¹²⁸

- Supporting the identification and arrest of people wanted for criminal offences;
- Supporting the identification of people about whom there is intelligence to suggest may pose a risk of harm to themselves or others;
- Supporting the use of targeted preventative policing tactics in areas where intelligence suggests violent crime may be committed.

South Wales Police claims that OIFR should not replace traditional identification methods, such as conversing with the public, and should only be used following an interaction between an officer and a data subject. Both a reason and a legal ground are required to justify the use of OIFR.

125 Freedom of Information Request to South Wales Police, FOI288/23, 23rd March 2023

126 Facial Recognition Technology, Cheshire Police, accessed 27th March 2023, <https://www.cheshire.police.uk/police-forces/cheshire-constabulary/areas/cheshire/about-us/about-us/facial-recognition-technology/>

127 OIFR Policy, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-policy-v0.4.pdf>

128 Ibid.

The reasons listed by South Wales Police to use OIFR are:¹²⁹

- The Subject is unable to provide their details [e.g. if they are deceased, unconscious, incapacitated due to drink, drugs or mental health, or due to age barriers].
- If the Subject cannot provide their details due to their mental health or an age barrier, or there is a clear language barrier preventing this being achieved, the Operator is to undertake reasonable lines of enquiry (such as the identification of an appropriate carer or interpreter) to facilitate identification before using OIFR.
- The Subject has refused to provide their details.
- It is reasonably suspected that the Subject has provided false details.

The legal grounds for OIFR use are if the subject is reasonably suspected to:¹³⁰

- Have committed a criminal offence or being unlawfully at large with further police action required.
- Further police action may include arrest or a need to verify details, depending on the criminal investigation.
- Be subject to bail conditions, a court order or other restrictions that would be breached if they were at the location at the time.
- Be a missing person deemed at increased risk.
- Increased risk is defined as being at College of Policing medium level or above, e.g. the risk of harm to the subject or public is likely but not serious
- Present a risk of harm to themselves or others.
- Be deceased (or confirmed deceased)

South Wales Police's documents lay out the restrictions on how officers can use OIFR. Force cannot be used to obtain a probe image, a stance which is audited by Body Worn Video footage. They also clarify that failing or refusing to confirm one's identity is not a criminal offence in itself and does not render someone liable for arrest, and a lawful basis is still required to make use of OIFR.

Officers are not limited to public spaces when using OIFR - they can also make use of phone-based facial scanning in private spaces they are lawfully in, taking into account the subject's expectation of privacy.¹³¹ They should also inform subjects they are about to

129 Standard Operating Procedure for the Overt Use of OIFR, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-sop-v0.6.pdf>

130 Standard Operating Procedure for the Overt Use of OIFR, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-sop-v0.6.pdf>

131 Standard Operating Procedure for the Overt Use of OIFR, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-sop-v0.6.pdf>

be subjected to an OIFR scan and lay out both the reason and the grounds, and record any concerns expressed by the person about the use of a biometric scan.

The process of how an OIFR facial scan works is laid out in the police Standard Operating Procedure:

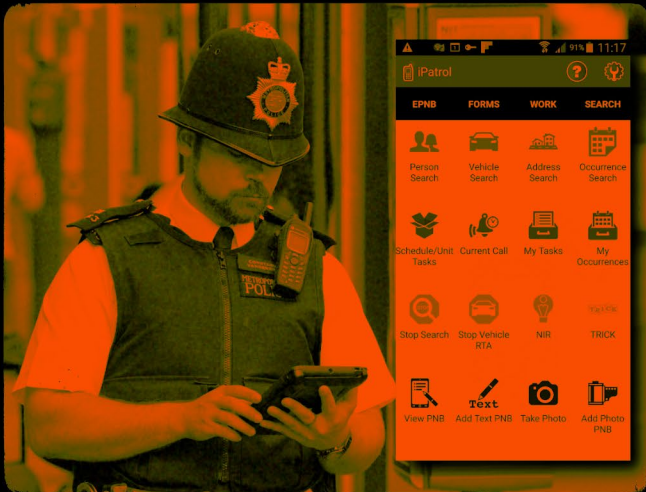
1. An officer opens the "iPatrol" app on their mobile phone and selects the facial recognition function
2. They are then prompted to select both the reason and the grounds for the OIFR scan, as well as the watchlist the face is being searched against
3. The officer must record the location of the OIFR scan, either by entering an address or using the phone's GPS
4. After the justification and location are submitted the officer can then take a probe image of the member of the public
5. Once the photograph is taken it is analysed by facial recognition algorithms and compared against the watchlist
6. Up to six potential matches are displayed in the app, with photos shown stripped of any personal details
7. If an officer thinks one of the results is a potential match they can select it to see further details
 - a) These details are the same as would be displayed if the person was identified by other means and the database searched via the iPatrol app.
 - i. This could include name, date of birth, address, any distinguishing marks and tattoos, any warnings on the system and the outcome of any prior interactions
8. If a potential match is selected the officer is then required to then press 'match', or 'no match' below the personal details to record the veracity of the potential match
 - a) If none of the potential matches is deemed to be correct the officer can hit "dismiss all", and must then record the age, gender and ethnicity of the member of the public in the app.

Once a potential match is confirmed the OIFR process is over and any action taken is

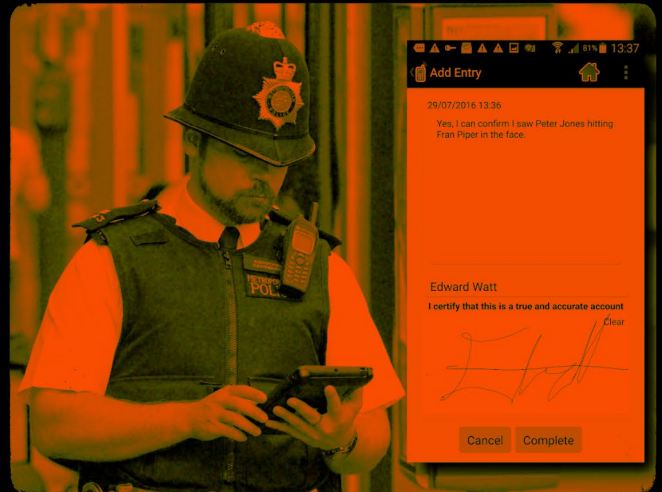
down to the officers involved themselves. This is a key reason the police maintain the deployment of OIFR is not an automated decision subject to Article 22 of the GDPR. In the Legal Mandate outlining the use of OIFR in Wales, the two forces suggest the technology could be used in a range of contexts, including “large crowded events known to be frequented by sexual predators” and “assemblies and demonstrations.”¹³²

¹³² OIFR Legal Mandate, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-legal-man-date-v0.4.pdf>

Officer opens
"iPatrol" app



Prompted to select reason
& grounds for OIFR scan



Officer must record
location of OIFR scan



Officer can then
take a probe image



Photo then analysed and compared against watchlist



Up to six potential matches are displayed in the app



Officer can select potential match to see further details



Officer required to press 'match', or 'no match'



Image Reference Database

South Wales Police and Gwent Police operate a joint database of images that are used as the reference list for OIFR, which is made up of both forces' custody image databases and missing person lists.^{133,134} The reference photo database will not be stored on officers' phones - instead, a connection to the internet and police servers will be required to conduct a face scan using OIFR.

Between them, the two forces hold more than 600,000 custody images, many of which will be held unlawfully as outlined in the chapter on PND Facial Searching.^{135,136,137} When justifying using the entire custody database for OIFR searches, the South Wales Police DPIA claims that it was necessary and proportionate to do so, because it is not technically feasible to segment the custody image database into smaller groups, such as those wanted for bail breaches or subject to outstanding arrest warrants.

South Wales Police does acknowledge that it is feasible to segment the database on demographic grounds, such as age or gender. However, it still refused to do this and insisted on running the biometric scan against the whole 600,000-person plus database, claiming that if officers had to guess at someone's demographic categorisation if the subject refused to cooperate, errors could be made and relevant people excluded from a search.

The DPIA also briefly acknowledges the risk of using custody images of innocent members of the public but minimises the issue that these photographs continue to be retained unlawfully – stating that it is not unique to South Wales or Gwent and that automatic deletion is not being pursued as the effort required to comply with the RJ High Court ruling “has not been deemed proportionate”.¹³⁸

133 Standard Operating Procedure for the Overt Use of OIFR, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-sop-v0.6.pdf>

134 Data Protection Impact Assessment for OIFR, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-dpia-v0.5.pdf>

135 Facial Recognition Technology, South Wales Police, accessed 8th April 2023, <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/>

136 Freedom of Information Request to South Wales Police, FOI79/23, 6th March 2023

137 Freedom of Information Request to Gwent Police, FOI2023/25904, 23rd February 2023

138 Data Protection Impact Assessment for OIFR, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-dpia-v0.5.pdf>

Use Statistics

Although both South Wales Police and Gwent Police were supposed to trial OIFR, when asked for results from these trials only South Wales returned data with Gwent Police claiming technical issues stopped them from using the app.¹³⁹

The South Wales Police data found that its officers had used OIFR 42 times in the 3-month trial. Of these 20 returned a match, 16 did not, four searches were abandoned and two were marked incomplete.¹⁴⁰

Reason	Number
Unable to Provide Details	17
Suspected False Details	18
Refused to Provide Details	7

Grounds	Number
Suspected Offence	30
Suspected Missing Person	9
Deceased	2
Suspected To Suffer Harm	1

Outcome [ALL OIFR]	Number
No Further Action	16
Arrest	11
Deceased	3
Incomplete	2
Report for Summons	4
Non Criminal Disposal	2
Missing Person Confirmed	1
Refused to Consent	1
None Recorded	2

¹³⁹ Freedom of Information Request to Gwent Police, FOI2022/25016, 6th April 2022, <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/>

¹⁴⁰ Freedom of Information Request to South Wales Police, FOI2022/317, 14th June 2022

Outcome	Number [MATCH]	Number [NO MATCH]	Number [ABANDONED]	Number [NOT RECORDED]
No Further Action	7	8	1	0
Arrest	8	3	0	0
Deceased	1	2	0	0
Incomplete	0	0	0	2
Report for Summons	2	2	0	0
Non Criminal Disposal	1	1	0	0
Missing Person Confirmed	1	0	0	0
Refused to Consent	0	0	1	0
None Recorded	0	0	2	0

No further action was taken in seven of 20 searches where there was a match [35 per cent] and eight of 16 occasions where there was no match [50 per cent].

Forty per cent of occasions [seven of 17 times] when a match was obtained, and the facial scan was justified by an officer who suspected an offence saw no further action. This suggests that OIFR was frequently being used despite the police not having sufficient grounds.

OIFR has been used on several occasions when officers claimed that someone was unable to provide details, while the grounds were a suspected offence [nine of the 17 times] according to detailed use data from SWP.¹⁴¹ The implication of this is either that a key use case of OIFR is on people who are incapacitated, or that reasons and grounds are not being properly recorded in all cases.

141 OIFR Data, Freedom of Information Request to South Wales Police, FOI317/22, 14th June 2022

Officer defined ethnicity	Total
Arabic/North African	4
Asian	4
Black	4
Unknown	3
White [North European]	25
White [South European]	2
Total	42

Age range	Total
10-17	6
18-30	21
31-60	15
Total	42

Gender	Total
Female	3
Male	39
Total	42

The ethnicity breakdown of OIFR use shows concerning disproportionality. In the South Wales Police area around 8.5 per cent of people are from an ethnic minority background.^{142,143} However, 30.7 per cent of OIFR searches where police defined the subject's ethnicity were conducted on people from an ethnic minority background.¹⁴⁴ People from a non-white background are almost four times as likely to be subjected to an OIFR scan than white people when accounting for the ethnic make-up of the South Wales population.

As a comparison, the difference between the ethnic breakdown in the community and among OIFR searches is a similar disproportionality to the Metropolitan Police's use of stop and search, which has widely been condemned as racist.¹⁴⁵

Arrest data for South Wales Police further demonstrates disproportionality – 81.6 per

¹⁴² Ethnicity By Area and Ethnic Group in Year To 30th June 2022, StatsWales, accessed 30th March 2023, <https://statswales.gov.wales/Catalogue/Equality-and-Diversity/Ethnicity/ethnicity-by-area-ethnic-group>

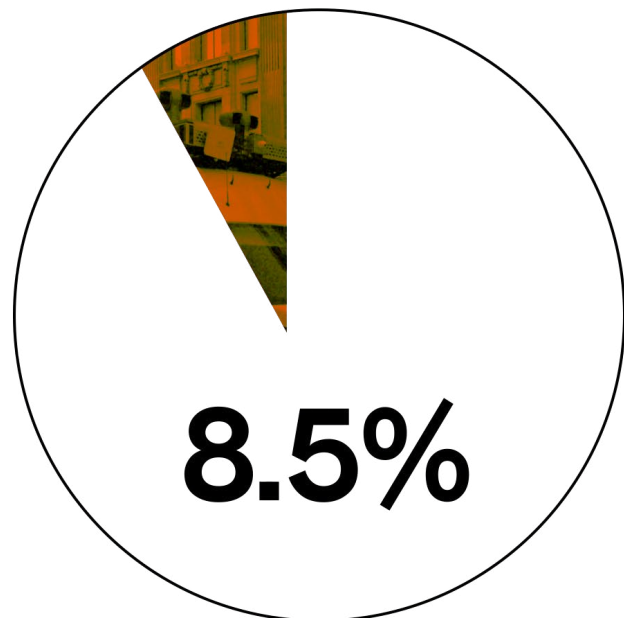
¹⁴³ Data for six of the seven local authority areas, excluding Merthyr Tydfil as no data was held, shows 107,700 people of an ethnic minority background of 1,273,000 total people.

¹⁴⁴ 12 of the 39 OIFR uses where ethnicity was identified were conducted on Black, Asian or Arabic/North African people.

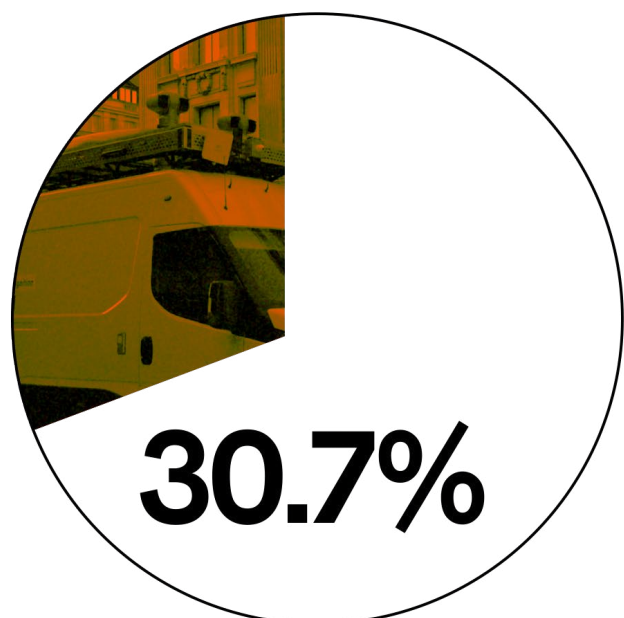
¹⁴⁵ Met Police 'disproportionately' Use Stop And Search Powers On Black People, The Guardian, 26th January 2019, <https://www.theguardian.com/law/2019/jan/26/met-police-disproportionately-use-stop-and-search-powers-on-black-people>

cent of people arrested by South Wales Police in 2020/1 were white, while just 18.4 per cent were of an ethnic minority background.¹⁴⁶ The proportion of OIFR facial searches was almost twice as high for non-white people as the proportion of arrests they make up in the area.

**PROPORTION OF PEOPLE
IN SOUTH WALES WHO
ARE FROM AN ETHNIC
MINORITY BACKGROUND**



**PROPORTION OF
OIFR SEARCHES ON
PEOPLE FROM AN ETHNIC
MINORITY BACKGROUND**



There is also a clear gender disparity in the use of OIFR with women making up around 7.1 per cent of OIFR uses, which is below even the arrest rate of women who make up 15 per

¹⁴⁶ Arrests, Ethnicity Facts and Figures, GOV.UK, 12th May 2022, <https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/number-of-arrests/latest#download-the-data>

cent of arrests across the UK.¹⁴⁷

Comparison to Other Street Biometrics

Another widely used form of “on-the-spot” biometric processing is the use of mobile fingerprint scanners . Most police forces deploy small fingerprint scanners which attach to a mobile phone for use either when there is reasonable suspicion of an offence being committed and someone refuses to give their name, or if an officer believes they have been given a false name.¹⁴⁸

Although biometric identification should not be the first option, fingerprints can be taken by force if necessary but this is not recommended. Police mobile fingerprint scanners have access to both IDENT1 [law enforcement] and IABS [immigration] databases and some police forces advise officers to search both databases by default to make sure the search is “thorough”.¹⁴⁹ As well as returning any identifying details, or police-held information, this could lead to someone being detained for residency or visa issues as police are required to flag anyone of interest to Home Office Immigration Enforcement.

These scanners are meant to be used when there is reasonable suspicion of a person committing an offence, or they have either not provided a name to police or police suspect a name they have given is false.

Stop The Scan, a campaign organised by the Racial Justice Network and Yorkshire Resists, which opposes the use of street biometrics, has expressed concern about the subjectivity of the decision to conduct a fingerprint scan due to doubt about the name someone has given. This power in particular appears to be exacerbating racial disparities in the use of suspicion-light surveillance powers. Data shows that black people are four times more likely than white people to be stopped and have their fingerprints scanned, while Asian people are twice as likely.

Many of the concerns about the already widely-used fingerprint scanners apply to mobile-phone-based facial recognition. The only major difference in operating procedure as it stands is that force cannot be used to take a photograph for facial recognition - but as a photograph can easily be taken without contact, or force, without consent it has significant potential for disproportionate use.

¹⁴⁷ Women and the Criminal Justice System 2019, Ministry of Justice, accessed 31st March 2023, <https://www.gov.uk/government/statistics/women-and-the-criminal-justice-system-2019/women-and-the-criminal-justice-system-2019>

¹⁴⁸ Mobile Fingerprint Identification Policy, Sussex Police, accessed 30th March 2023, <https://www.sussex.police.uk/SysSiteAssets/foi-media/sussex/policies/mobile-fingerprint-identification-policy-survey-and-sussex-1191.pdf>

¹⁴⁹ Ibid

Operator initiated facial recognition has the potential to reshape police encounters with members of the public, giving officers access to powerful, on-demand mobile surveillance technology that uses our faces to unlock any records held about us. Whether at protests, on the roads or during stop and searches, police officers could, depending on the size of image reference libraries used, have the ability to instantly identify people they interact with. The scenarios that police forces envision using OIFR in, protests and large public gatherings, suggest this will not be a strictly targeted tool, used only in exceptional cases where it is essential but impossible to identify someone, but rather one that risks overuse. The widespread rollout of this technology would see a new era of technology-led policing, where biometric face scans and database checks become routine on the streets of Britain. It is a technology that has to the potential to create a nation of “walking ID cards”.

As with other forms of facial recognition, police use of OIFR represents an interference with the right to privacy, which police must demonstrate is necessary and proportionate. South Wales Police suggest the use of the technology is necessary as it “is a tool that helps [...] to discharge its operational responsibilities”. This is a low bar that does not specifically engage with why OIFR is specifically necessary. An example given is that it could be used at “large crowded events known to be frequented by sexual predators in an attempt to identify and prevent similar attacks”.¹⁵⁰ If those being sought by the police are known individuals, present at known locations, it is not clear that OIFR is strictly necessary when considering traditional methods (spotter cards, or super recognisers, for example). However, there is a risk that such a technology could be used widely and indiscriminately to scan individuals in the crowd. Such a use of the technology would entirely undermine the proportionality of its use, as well as making it highly inefficient.

Police officers in the UK have no “stop and account” powers, meaning they cannot require an individual to give their name, address or any account of what they are doing in the area. Individuals are only required to identify themselves if they have been informed that they are suspected of committing an offence. The grounds for an OIFR scan, as with other police uses of facial recognition, go beyond suspected criminal activity and include nebulous categories of presenting “a risk of harm to themselves or others”. This broad category gives police forces vast scope to utilise this technology in a range of non-crime related situations.

South Wales Police claim that their use of the technology is proportionate as officers will give “consideration as to the effectiveness and intrusiveness of other viable methods that could give the same result” and state “the use of OIFR to confirm or eliminate a person’s identity may be less intrusive to arresting the individual in order to later

¹⁵⁰ OIFR Legal Mandate, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-legal-mandate-v0.4.pdf>

confirm their identity at a police station”.¹⁵¹ Officers can only arrest an individual if they are suspected of an offence, and cannot do so purely to identify them at a station. OIFR does not therefore, represent a more proportionate policing intervention, as it takes place pre-arrest and can be undertaken for non-crime purposes. If an individual is reasonably suspected of committing an offence, their identity can be established if they are arrested. OIFR, however, represents a new category of policing intervention between suspicion and arrest, which is deeply intrusive and unnecessary.

OIFR, as with other forms of police use of facial recognition, poses a risk to freedom of expression and assembly. South Wales Police suggests that OIFR could be used “in policing an assembly or demonstration, particularly where there is an intelligence case supporting there being a risk to public safety”, noting that “OIFR can support Operators by efficiently identifying suspects for violence in crowded locations where it might otherwise be difficult to identify them”.¹⁵² It is not clear how police expect OIFR to assist in locating wanted individuals in crowds unless large numbers of demonstrators are scanned. Given that officers must engage with an individual before they are subject to a biometric scan, this seems highly impractical and will doubtless have a significant chilling effect on individuals’ willingness to attend protests.

Police forces do recognise that people may expect privacy in a crowd, and that using OIFR may “deter members of the public from exercising their right to freedom of assembly and freedom of expression afforded by the Human Rights Act”.¹⁵³ However, these threats to protest rights are justified with the questionable assertion that OIFR is used to “enable an assembly that might otherwise be disrupted” and to help the public “safely undertake their assembly”. Claiming that intrusive surveillance makes people more likely to protest disregards considerable evidence to the contrary.¹⁵⁴

As with RFR, OIFR searches forces’ custody images, as well as images of missing persons. The same data protection and privacy concerns arise from the mass retention of facial images of unconvicted individuals as previously outlined; innocent people will have their biometric data processed every time a search is undertaken and are also at risk of being wrongly flagged by the technology. The police argue that the lack of technical capacity to automatically delete these unlawfully held images makes this processing proportionate.¹⁵⁵

151 OIFR Legal Mandate, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-legal-man-date-v0.4.pdf>

152 OIFR Legal Mandate, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-legal-man-date-v0.4.pdf>

153 Data Protection Impact Assessment for OIFR, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-dpia-v0.5.pdf>

154 See footnote XX. Get Maddie to confirm which one when final changes have been confirmed.

155 Data Protection Impact Assessment for OIFR, South Wales Police, accessed 28th March 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-dpia-v0.5.pdf>

There is no legal precedent to support the argument that the failure to conduct adequate technical or administrative work, resulting in excess data retention and access, makes subsequent excessive data processing "proportionate". On the contrary, such processing incurs multiple data protection breaches and privacy interferences across multiple stages. Police forces should not be deploying any form of facial recognition while issues surrounding the retention of facial images of innocent people remain unresolved.

Our analysis has found serious racial bias in how OIFR is currently being used by South Wales Police: people from a non-white background are almost four times as likely to be subjected to an OIFR scan than white people. This tallies with other policing practices, such as fingerprint scanning and stop and searches, where people of colour are more likely to be subject to policing interventions and surveillance. The use of this technology poses a threat to the privacy of all citizens, but it is unacceptable that it is being utilised in a way that contributes to the over-policing of people of colour. Given recent reports of institutional racism in UK policing, it is alarming that South Wales Police believes this discriminatory use of OIFR does not warrant a pause in its use and further investigation.

There is also a significant risk of discrimination on the grounds of nationality, age, and mental health when using OIFR. South Wales Police state that an OIFR scan can be undertaken if an individual is unable to provide their details, meaning those who cannot speak English or who struggle to communicate with police officers due to their age or mental capacity will be far more likely to be subject to an OIFR scan. This two-tier approach to policing, where those with communication issues, or disabilities are subject to intrusive facial scans at a higher rate, is deeply troubling and discriminatory.

RECOMMENDATION: The use of operator-initiated facial recognition by police forces should be prohibited as no case has been made as to why such power is strictly necessary and it poses a significant risk to the rights of the British public. Individuals can be identified at police stations if there is a lawful reason for their arrest.

Key UK Reports and Rulings

In the five years since Big Brother Watch published its initial Face Off report, there have been several landmark reports published and rulings made criticising and curtailing the use of FRT, including the Bridges case. These publications have been key points in the ongoing conversation surrounding FRT and are summarised below, although the full reports are necessary reading for the fullest possible understanding of each.

Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology 2019¹⁵⁶

Professor Peter Fussey and Dr Daragh Murray's 2019 report [referred to hereafter as the "Essex report"] was commissioned by the Metropolitan Police as an independent analysis of its then-trials of facial recognition, although it was funded by the Economic and Social Research Council. The academics from the University of Essex Human Rights Centre concluded that it was "highly possible" that the Met's use of LFR would be found unlawful if a legal challenge was brought against it.¹⁵⁷ Despite the Essex report being commissioned by Scotland Yard, the Metropolitan Police attacked the authors in statements following its publication, labelling it as "negative and unbalanced" even though it was written by independent academics.

The researchers observed six of the Met's trial deployments from June 2018 to February 2019, covering the Westfield shopping centre in Stratford, Soho in central London and Romford town centre, to the east of the capital. They had access to the deployments themselves, briefing meetings and documents surrounding the deployments. The authors sought to clarify that their findings related to the Met's use of LFR specifically, which was then described as a trial.¹⁵⁸

Professor Fussey and Dr Murray identified some major concerns about how the Met Police was making use of LFR, which focussed on four key areas:

- Met Police research processes, which the Essex report said focussed on the technical side of LFR [such as accuracy] while being unclear on non-technical objectives such as establishing whether LFR is a useful policing tool
- The Met did not have an explicit legal basis to use LFR, while the implicit legal basis

¹⁵⁶ Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, Peter Fussey and Daragh Murray, University of Essex Human Rights Centre, July 2019, <https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf>

¹⁵⁷ 81% Of 'Suspects' Flagged By Met's Police Facial Recognition Technology Innocent, Independent Report Says, Sky News, 4th July 2019, <https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941>

¹⁵⁸ Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, Peter Fussey and Daragh Murray, University of Essex Human Rights Centre, July 2019,

was inadequate to establish that the use of LFR was “in accordance with the law”.¹⁵⁹

- The lack of explicit legal authorisation of LFR is a reason why the authors argued that it was likely that LFR could be found unlawful in a legal challenge.
- The Met failed to effectively establish whether using LFR was “necessary in a democratic society”, which is a requirement of human rights law.
- The authors found that the Met’s trial deployments may not be seen as necessary in a legal challenge and that the force failed to account for the intrusive nature of biometric data processing.
- Operational deployment concerns include inconsistency in the adjudication process concerning matches, a presumption towards intervening with possible matches, issues with these interventions and difficulties obtaining the consent of people affected.

Across the six deployments observed by the authors of the Essex report, they found that only eight of the 42 matches on the LFR system could be verified as being correct, with 16 of the 42 being rejected by officers as “non-credible” and a further 14 people who were stopped by police turning out to be someone else. A further four people who were flagged as potential matches were not stopped by police, often due to getting lost in the crowd.

The Essex report found that even when discounting the 16 alerts deemed to be “non-credible” by officers and the four alerts that police did not intervene with, 63.64 per cent of LFR alerts were false positives [14 of 22 interventions following a match], and just 36.36 per cent [eight verified matches] were true positives. The authors use the precision figure, similar to that used by Big Brother Watch, to measure LFR accuracy [the proportion of false matches as a percentage of total matches] rather than the police’s preferred metric of the proportion of false matches of the total number of faces scanned.

The report also described that much of the data used to build the watchlists, which are a fundamental part of LFR deployments, was often old. Some people were stopped following an alert despite their case already having been dealt with – something Big Brother Watch has also observed, while others were put on watchlists with little reason – which the authors said created “significant ambiguity” about the real purposes for deploying LFR.¹⁶⁰

The Metropolitan Police ultimately rejected the findings of the independent report it commissioned, declaring just months later that LFR was moving from trial use to operational deployments.¹⁶¹ Despite this, many of the major concerns raised by Professor Fussey and

¹⁵⁹ No law authorising the use of LFR has ever been passed, instead, the Metropolitan Police relies on a host of other laws including common law crime prevention powers, the Human Rights Act 1998, the Protection of Freedom Act 2012 and the Regulation of Investigatory Powers Act 2000 to justify its use of the technology.

¹⁶⁰ New Report Raises Concerns Over Met Police Trials Of Live Facial Recognition Technology, University of Essex, 3rd July 2019, <https://www.essex.ac.uk/news/2019/07/03/met-police-live-facial-recognition-trial-concerns>

¹⁶¹ Police Force To Roll Out ‘81% Inaccurate’ Live Facial Recognition, Sky News, 24th January 2020,

Dr Murray have not been addressed and the Met continues to push its own interpretation of the statistics in an attempt to deny the dangerous inaccuracies and threats to privacy involved in biometric surveillance.

In light of the authors' unprecedented access, the concerns highlighted in the Essex report are a damning indictment of the Met's deployment of LFR and although the force rejected the independent findings, it is a key document in the conversation around LFR in the UK.

R (Bridges) v South Wales Police, Court of Appeal Ruling, 2020

R (Bridges) v South Wales Police [referred to hereafter as the Bridges case] is a 2020 ruling from the Court of Appeal, which was the first significant legal challenge to the use of facial recognition technology in UK policing. It was brought by Dr Ed Bridges, an activist and former Liberal Democrat councillor in Cardiff, who was supported by Liberty.¹⁶²

The Court of Appeal, overturning a High Court ruling, found that South Wales Police's use of LFR was unlawful and interfered with Mr Bridges' right to privacy under Article 8 of the European Convention on Human Rights.

The case concerned two LFR deployments in which Mr Bridges was subject to a biometric scan by the facial recognition system, one outside a busy shopping centre in the run-up to Christmas 2017 and the second at a protest against an arms fair at the city's Motorpoint Arena in 2018. He challenged the use of LFR arguing that it breached data protection and equality laws, and his right to privacy.

Dr Bridge's challenge was initially rejected by the High Court, but he appealed the lower court ruling on five counts – and the Court of Appeal ruled in his favour on three of these:¹⁶³

- a) Privacy rights, under Article 8 of the ECHR, were breached because of the insufficient legal framework governing LFR, leaving officers on the deployment with too much discretion in how they used the biometric technology
- b) Equalities law - the Public Sector Equality Duty [PSED] was breached because police failed to do all they could to address the risk of discrimination arising from the algorithms that could be biased on grounds of gender or race

<https://news.sky.com/story/metropolitan-police-to-make-81-inaccurate-live-facial-recognition-operation-al-11916479>

¹⁶² Facial Recognition Use By South Wales Police Ruled Unlawful, BBC News, 11th August 2020, <https://www.bbc.co.uk/news/uk-wales-53734716>

¹⁶³ R (Bridges) v Chief Constable of South Wales Police, EWCA Civ 1058, Court of appeal, 11th August 2020, <https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf>

- c) Data Protection Impact Assessment [DPIA] – Police were found to have breached Section 64 of the Data Protection Act 2018 due to the DPIA conducted about the use of LFR being deficient

Dr Bridges is a landmark ruling in that it found South Wales Police's use of LFR was not "in accordance with law"¹⁶⁴. Police have since developed new policies and conducted bias studies to justify their resumed use of live facial recognition in the UK.

Equitability Study, National Physical Laboratory, 2023¹⁶⁵

In the summer of 2022 the National Physical Laboratory [NPL], a government-funded metrology institute, evaluated the equitability of the different forms of facial recognition used by the Metropolitan Police and South Wales Police; live, retrospective and operator-initiated. It was jointly funded by the Home Office and Metropolitan Police.¹⁶⁶

The findings were published in April 2023, close to the finalisation date for this report meaning that work to understand, analyse and respond to its findings is still ongoing but it is nonetheless important to acknowledge the NPL report and highlight some initial concerns with it.

The report author, Dr Tony Mansfield, outlined his key findings as:

LFR

- A True Positive Identification Rate¹⁶⁷ [TPIR] of 89per cent when the LFR system was running at a match threshold of 0.6¹⁶⁸, which is NEC [the system manufacturer's recommendation].
- No statistically significant bias for age, gender or a combination of the two in LFR when running at a match threshold of 0.6 or above
- At thresholds of 0.58 and 0.56, the system was found to perform statistically significantly worse for black people.
- A False Positive Identification Rate [FPIR]¹⁶⁹ of one in 6,000 [0.017per cent] when

¹⁶⁴ Facial Recognition Technology No "In Accordance With Law", UK Human Rights Blog, 13th August 2020, <https://ukhumanrightsblog.com/2020/08/13/facial-recognition-technology-not-in-accordance-with-law/>

¹⁶⁵ Facial Recognition Technology In Law Enforcement Equitability Study, Dr Tony Mansfield, National Physical Laboratory, March 2023, <https://science.police.uk/site/assets/files/3396/frt-equitability-study-mar2023.pdf>

¹⁶⁶ Ibid

¹⁶⁷ The TPIR is the number of people who were correctly matched by the LFR system, compared against the amount who should have been – for example if 100 people on the list passed the camera and 50 led to alerts, the TPIR would be 50%.

¹⁶⁸ The match threshold is the similarity score of the probe image compared against any image on the watchlist above which the LFR system generates an alert

¹⁶⁹ The FPIR is the number of false matches as a percentage of the total faces seen, for example, if 100

running at a threshold of 0.6 and on a 10,000-person watchlist.

RFR and OIFR

- The TPIR for both operator-initiated and retrospective facial recognition was 100per cent, meaning that the system returned the correct person every time a photograph of somebody in the database was searched.
- From this, it follows that there is no demographic bias in these tools, as they had perfect TPIR scores.

Following the report's publication the Metropolitan Police claimed it was a "significant report for policing" which vindicated their push to continue using live facial recognition in London, claiming it will help them tackle crime [despite the report not assessing the technology's operational utility].¹⁷⁰ There are significant concerns following the report that both the Metropolitan Police and South Wales Police will ramp up their use of FRT. Indeed, the Metropolitan Police used LFR three times in the month of April 2023.

However a close reading reveals methodological issues and serious demographic bias issues with the facial recognition algorithm.

The study identified a statistically significant difference between the false positive rate of black and non-black subjects during the use of LFR, specifically when the confidence threshold to generate a match was set below 0.6. This alarming finding provides yet more evidence, following observational data and the NPL report in 2020, that the LFR algorithm has a serious demographic accuracy bias. Documents seen by Big Brother Watch show that the Met Police has frequently operated LFR below a 0.6 confidence threshold and set the threshold as low as 0.55, in 2017 and 2018, while its LFR policy suggests that the threshold is variable.¹⁷¹

The report states that, with a 0.6 threshold, there are still demographic accuracy differences across race and gender but that these are not statistically significant. We would posit the obvious point that by generating fewer matches, fewer demographic differences will be measurable in the sample. Given the algorithm is evidenced to have demographic accuracy issues, we are not at all satisfied that a higher confidence threshold is an appropriate or sufficient mitigation to avoid potential discriminatory effects on the population when LFR is in wider use.

Specifically on retrospective facial recognition Dr Mansfield outlines a key difference between the testing environment, which found a 100per cent TPIR rate, and real-world

people walked past the camera and there was one false match, the FPIR would be 1%. As outlined elsewhere in this report Big Brother Watch, and independent experts, do not regard this as the best measure of FRT inaccuracy.

¹⁷⁰ Statement On Release Of Research Into Facial Recognition Technology, 5th April 2023, <https://news.met.police.uk/news/statement-on-release-of-research-into-facial-recognition-technology-464791>

¹⁷¹ Freedom of Information Request to the Metropolitan Police, FOI2018110000706, 23rd January 2019

deployment. The report states that high-quality images were used both for the reference and probe images, whereas the reality is that in policing use, many of the images [particularly probe images from grainy CCTV] will be of poor quality, which may well lead to much poorer performance. It also states the images captured for testing purposes were taken just days apart, rather than the potential months or years between a RFR probe image and the photograph of a person held by the police – something which would also degrade performance.

A further consistent thread through the report is the argument that the bigger the watchlist, the greater the chance of false positives or biased outcomes [due to the greater number of comparisons made]. Yet the RFR and OIFR figures outlined in the report are based on a 100,000-person watchlist, which is far removed from how the technology is used in reality. RFR searches can be performed against entire custody photograph databases – with the Met Police’s database containing 3.6 million images and the combined South Wales/Gwent database totalling 600,000 images.¹⁷² Realistic watchlist sizes were not used in the study of RFR and OIFR, limiting the report’s findings.

There is also no consideration given to false results in OIFR and RFR, as Dr Mansfield outlines that instead of generating an alert police are given a suite of potential matches ranked by comparison score – meaning there is no definitive false positive. However, given the known phenomenon of human bias towards computer recommendations, and the police’s stated intent to require people to prove a negative [that they are not the person identified], the NPL report fails to account for what could be dangerous errors if someone is accused of being someone they are not.¹⁷³¹⁷⁴

The report acknowledges that this sometimes occurs, with some results having a similarity score of 0.6 despite being images of different people, but does little more to investigate this. It also outlines in the discussion that people of colour disproportionately made up the number of false matches [that is the occasions where the top result was of a different person than the probe image], and this disparity could be exacerbated in operational deployments due to the use of poorer quality images and the time-gap between the probe and reference images in real-world scenarios.

The “impartial” study by Dr Mansfield, who we have seen attending and contributing to the design of Met Police LFR trials since 2018 and who co-authored a 2020 report on LFR with the Met Police, provides some technical analyses of LFR rather than operational. The issue of the demographically biased algorithm performance, in an operational setting,

172 Facial Recognition Technology, South Wales Police, accessed 8th April 2023, <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/>

173 Automation Bias In Intelligence Time Critical Decision Support Systems, M.L Cummings, Intelligent Systems Technical Conference, American Institute of Aeronautics and Astronautics, 20-22 September 2004, <https://arc.aiaa.org/doi/10.2514/6.2004-6313>

174 Live And Retrospective Facial Recognition Technology, Caroline Russell, YouTube, 22nd December 2021, https://www.youtube.com/watch?v=bGv5_OCz4h0

is compounded by risks of human discrimination in the compilation of watchlists and in subsequent police interactions. This has not been accounted for by police forces or in the "scientific" NPL reports.

Further analysis of the NPL report is expected in the coming months but the initial analysis both by Big Brother Watch and academic experts suggests that the significant issues around accuracy and bias that it raises need urgently addressing.

Schools

The use of biometrics in schools to perform relatively straightforward tasks has become a significant threat to childrens' data rights and privacy. Fingerprint-based systems are used in a large proportion of secondary schools, mostly to identify pupils in the school canteen, but also for other purposes such as library access.¹⁷⁵ A number of schools are now introducing facial recognition systems, typically focused on lunch payments, to replace fingerprints or swipe cards.

Cashless payment systems for school canteens have become the dominant payment method. Parents top up their child's account online, which is charged for the meals they purchase in the canteen. Swipe cards, fingerprints and increasingly facial recognition are used to identify the correct account on the school system so the right person is charged for the meal.

These facial recognition systems operate by capturing a reference image of a child and associating it with their account. A camera in the canteen then takes an image of the child as they purchase their food, and the software matches the biometric faceprint of this image against the school database to identify the child present. A cashier then charges the account.

Schools that have adopted facial recognition systems cite several different reasons for processing biometric data for the simple task of facilitating lunch payments. These have included claims around cost, speed and even pupil safety, e.g.:^{176,177}

- A faster lunch service
- COVID-19 hygiene, as facial recognition is contactless so does not require contact with a fingerprint reader
- Facial recognition is more efficient and will allow schools to offer "wholesome, healthy and enjoyable food at the lowest cost"¹⁷⁸

Although Big Brother Watch has not surveyed all schools about their use of facial recognition, from those with publicly accessible policies it appears that CRB Cunningham,

175 The State of Biometrics 2022: A Review Of Policy & Practice in UK Education, Defend Digital Me, May 2022, <https://defenddigitalme.org/wp-content/uploads/2022/05/The-State-of-Biometrics-in-UK-education-2022-v1.7.pdf>

176 Facial Recognition FAQs, Rivington & Blackrod High School and Sixth Form, accessed 20th March 2023, <https://www.rbhs.co.uk/Parents/facial-recognition/#:~:text=Simply%20visit%20ParentPay%20and%20click,be%20enabled%20on%20the%20system.>

177 Facial Recognition Letter, Carlton Academy, June 2021, <http://www.theacademycarlton.org.uk/uploads/images/file/Biometric%20consent%20-%20facial%20recognition%20-%20June%202021.pdf>

178 Payments, Queen Elizabeth School Luton, accessed 20th March 2023, <https://www.qesluton.co.uk/Payments/>

a company based near Edinburgh, is the most common supplier of the technology.

It has been reported that more than 60 schools are using the technology in total, from Plymouth to Nottingham, Gateshead and Bolton.¹⁷⁹ The growing number of schools using the technology and the enrolment rates suggest that facial recognition is becoming worryingly widespread and normalised in the UK education system.

Data from Defend Digital Me on school biometrics, in general, found that 85 per cent of pupils in schools using fingerprint readers enrolled on the system. We do not know how many children are similarly enrolled in facial biometrics for identification in schools.¹⁸⁰

North Ayrshire Council, in Scotland, attempted to roll out facial recognition in the canteens of nine of its schools in September 2021.¹⁸¹ However, there was significant pushback from Big Brother Watch which included letters to all the schools involved, parents, and the Biometrics Commissioner for England and Wales Prof. Fraser Sampson, who said schools should not use biometrics just because they can. Following the backlash and the launch of an inquiry by the Information Commissioner, the council halted the rollout.¹⁸²

Big Brother Watch's work around the subject of facial recognition for lunch payments found that information provided to parents on the use of facial biometrics was often incomplete, lacking key details about how the data would be processed. It also uncovered that some schools did not have effective consent procedures and made using facial recognition quasi-mandatory to allow children full participation in school life.

Guidance from the Information Commissioner issued in October 2022, following the North Ayrshire controversy, was clear about how schools could use facial recognition for cashless lunch payments.¹⁸³ The Commissioner stated that schools could only rely on explicit consent as a legal justification to process the biometric data involved in facial recognition, under Article 9 of the GDPR, and clarified that other justifications such as public task would not be sufficient as biometric data processing is unlikely to be deemed necessary for school catering purposes.

The guidance also points out that FRT poses risks in terms of bias and, given that children's biometric data is being processed, additional protection of their rights may be merited. Education authorities [mostly schools, but sometimes councils] are required to mitigate

179 Facial Recognition Cameras Arrive In UK School Canteens, Financial Times, 17th October 2021, <https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9>

180 The State of Biometrics 2022: A Review Of Policy & Practice in UK Education, Defend Digital Me, May 2022, <https://defenddigitalme.org/wp-content/uploads/2022/05/The-State-of-Biometrics-in-UK-education-2022-v1.7.pdf>

181 Ibid.

182 Schools Pause Facial Recognition Lunch Plans, BBC News, 25th October 2021, <https://www.bbc.co.uk/news/technology-59037346>

183 Case study: North Ayrshire Council schools - Use of Facial Recognition Technology, accessed 20th March 2023, <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/case-study/>

any potential data protection and discrimination risks and ensure that information on how data will be processed is made available in a child-friendly way.

As consent is the only justification that the ICO deems to be valid for facial recognition in school catering, schools are also required to make sure that there is no detriment to children or parents who opt out. The ICO cites examples, such as offering quicker service or lower prices to children enrolled in FRT systems, as those which are unacceptable.

Further guidelines from the Department for Education were issued in July 2022 which echoed the position taken by the ICO, including a requirement for non-detrimental provisions as alternatives to facial recognition, requirements for proper consent procedures and outlining schools' responsibilities relating to pupil's personal data.¹⁸⁴

Case Study

Leverhulme Academy Trust, which runs two high schools and a sixth form in Bolton, uses facial recognition in its canteen. It claims the benefits include it being contactless, speeding up the lunch service, saving students from carrying around a card and being secure. The Trust also says that the Covid-19 pandemic pushed them towards facial recognition due to fingerprint scanners risking virus transmission.¹⁸⁵

The FAQs on the Trust also claim that if a parent has permitted their child's fingerprint to be used in the cashless canteen then permission has been given for facial recognition to be used as well, as both are forms of biometric processing. This is incorrect in law and contradicts guidance from the ICO around consent to biometric processing, as any consent must "specify the nature of the special category data".¹⁸⁶ Consent must be specific for each type of processing.

In addition to the biometric faceprint the school also stores a photo of a child on the system for "added verification" - raising questions over whether facial recognition is necessary at all given that an ordinary photograph is subsequently used to identify the child - as it could be with a swipe card system.¹⁸⁷ This suggests that the facial recognition system is little more than a shortcut for staff to search the database to identify the correct account to charge.

184 Protection Of Biometric Data Of Children In Schools And Colleges, Department for Education, July 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092507/Biometrics_Guidance_July_2022.pdf

185 Facial Recognition In Our Schools, Leverhulme Academy Trust, accessed 20th March 2023, <https://www.leverhulmeacademytrust.org/Facial-Recognition/>

186 What Are The Conditions For Processing Special Category Data, Information Commissioners Office, accessed 20th March 2023, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions1>

187 Facial Recognition In Our Schools, Leverhulme Academy Trust, accessed 20th March 2023, <https://www.leverhulmeacademytrust.org/Facial-Recognition/>

The most alarming part of the Leverhulme Trust's policy is the fact that opting out of facial recognition is not free. In the FAQs it states parents/children who opt out of facial recognition must "purchase a card" as an alternative method of identification.¹⁸⁸ ICO consent guidance says that for consent to be freely given, refusing consent must not come with detriment to the data subject.¹⁸⁹

Meanwhile, an ICO case study on the use of facial recognition by schools in North Ayrshire says that alternatives, such as a swipe card, must be available without detriment – giving slower service or higher prices as examples. It is not clear whether the Trust's policy would also meet the threshold of detriment but charge for a swipe card evidently makes it more difficult to refuse consent.

¹⁸⁸ Facial Recognition In Our Schools, Leverhulme Academy Trust, accessed 20th March 2023, <https://www.leverhulmeacademytrust.org/Facial-Recognition/>

¹⁸⁹ What Are The Conditions For Processing Special Category Data, Information Commissioners Office, accessed 20th March 2023, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions1>

“While other countries around the world have banned children’s biometrics in educational settings as high risk, the UK was an early test-bed for widespread use”

- Jen Persson, Defend Digital Me

Commentary From Jen Persson, Defend Digital Me

"While other countries around the world have banned children's biometrics in educational settings as high risk, the UK was an early test-bed for widespread use. Since 2001 biometric systems using fingerprints have been used in schools to verify children's identity for buying canteen food, borrowing library books, and accessing buildings, lockers and printers.

"During the Covid-19 pandemic, some of the same companies began to promote facial detection and recognition products [FRT"].

"In October 2021, schools in Scotland adopted FRT for routine canteen cashless payment systems. Fraser Sampson, the Surveillance Camera and Biometrics Commissioner said at the time, "if there is a less intrusive way, that should be used." The ICO intervened and in January 2023 published its letter to North Ayrshire Council, with a case study "Using FRT in schools". While this did not constitute enforcement action, it concluded that since the process had been neither fully informed nor freely given, it was "likely unlawful".

"The Protection of Freedoms Act 2012 applies in England and Wales on consent and objections when processing a child's biometric data. While families must be asked for opt-in, at Defend Digital Me we believe practice remains fundamentally flawed, due to the power imbalance between the authority and child. Some school policies we have seen suggest that children entitled to Free School Meals are not given any choice.

"Progress is being made, albeit not enough. The Department for Education updated national guidance to suggest, "Facial recognition will often not be appropriate in schools and colleges if other options are available to achieve similar goals, like paying for school lunches," and, "Live facial recognition is not appropriate in schools or colleges."¹⁹⁰ And in March 2023 the Welsh Senedd backed a call for legislation led by Sarah Murphy, member for Bridgend, who summed up by saying, "it is really important that we do look at it through the lens of our values, our culture and ...the children's human rights, and the power dynamics and the power exchange that is happening here on our watch. As the Manic Street Preachers sing, 'If you tolerate this, then your children will be next.'^{191,192,193}

190 Protection of children's biometric information in schools, GOV.UK, accessed 1st April 2023, <https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools>

191 Welsh Senedd Debate under Standing Order 11.21(iv) — Biometric data in schools, 8th March 2023, <https://record.assembly.wales/Plenary/13262#A78251>

192 Senedd Backs Call For Legislation Over The Use Of Biometric Data In Schools, Deeside News, 12th March 2023 <https://www.deeside.com/senedd-backs-call-for-legislation-over-the-use-of-biometric-data-in-schools/>

193 Biometrics In Schools Briefing, Defend Digital Me, 2nd April 2023, <https://defenddigitalme.org/wp-content/uploads/2023/04/Biometrics-in-schools-briefing-2-April-2023.pdf>

Visas and Immigration

Biometric tools are becoming increasingly common in the UK's immigration system, being used both by the government and private companies. Using facial recognition to verify the validity of documents was a major part of the EU Settlement Scheme and is being used by companies such as Experian who perform "Right to Work" checks for employers. The Home Office is also seeking to roll out increasing uses of facial recognition at airports for border checks, to replace in-person passport controls.

Further, Big Brother Watch has discovered that London's Gatwick airport claims a facial recognition check is mandatory for passengers flying within the Common Travel Area (UK, Ireland, Isle of Man, Channel Islands) and that the airport is acting under a written order from the Home Office, issued under Schedule 2 of the Immigration Act 1971.¹⁹⁴ Any passenger who refuses a facial recognition scan is not allowed to fly – Gatwick Airport states, "further to our obligations pursuant to the Written Notice we operate a 'no fly' policy for any passengers who do not go through the facial recognition system in the designated areas."¹⁹⁵ The written notice is not publicly available. Big Brother Watch has sent a Freedom of Information request to the Home Office to seek a copy. Although there is no provision in Schedule 2 of the Immigration Act for written orders to be issued secretly, the Home Office has not published the written notice and told us it is currently considering our FOI request under the law enforcement exemption [s.31].

EUSS

The EU Settlement Scheme [EUSS] was a Home Office program that was implemented as part of the Brexit process, which was meant to allow the European Union [EU], European Economic Area [EEA] and Swiss citizens to remain in the country after the UK left the EU. Depending on certain criteria, people could receive "settled status" or "pre-settled status".

Applicants were required to submit several documents including evidence of their continuous residence in the UK and proof of identity, which was commonly verified through the use of facial recognition technology.

A mobile app called "EU Exit: ID Document Check" was released for Android and iOS devices supposedly to provide a quick and easy process for applicants to verify their identity documents. The four-step process was:¹⁹⁶

194 Biometric ID – Gatwick Airport, accessed 24th April 2023, <https://www.gatwickairport.com/at-the-airport/flying-out/security/biometric-id/>

195 Ibid.

196 EU Exit: ID Document Check, Apple App Store, accessed 16th March 2023, <https://apps.apple.com/gb/app/eu-exit-id-document-check/id1478914184>

- Take an image of your document
- Read the NFC chip in your document using your phone
- Scan your face using your phone
- Take a photograph of yourself for your digital status

The app used facial recognition technology to compare the image on the identity document with the image captured during the app's verification process. Although there were other methods available for applicants to verify their identities, biometric scanning was pushed as the default mode.

iProov, a British company, provided the technology underpinning the facial recognition process. The same company also powered the facial recognition verification of people enrolling on the NHS's vaccine passports app in 2022. Estimates from iProov claim that 3.1 million people used facial recognition during their EUSS application, out of a total of 5.3 million people who applied for the scheme.^{197,198} As the majority of applicants used the biometric option, after being pushed that way, any issues with the system will have impacted a huge number of people.

Anecdotal evidence collected by the Barrow Cadbury Trust found that there were difficulties for people with facial disabilities, such as claiming applicants' eyes were closed when they were not. A barrister also told the Trust that they experienced particular difficulties with the facial scan for some of their ethnic minority clients.¹⁹⁹ However, when the founder of iProov Andrew Bud spoke to Big Brother Watch about the vaccine passports scheme he claimed to not know about these issues and that they did not show up in internal statistics.²⁰⁰

The EUSS scheme has been largely wound down. It was the first major use of biometric recognition of faces against identity documents in the UK in relation to making residency and immigration decisions, and suggests that this is a tool the government may seek to use in the future.

197 EU Settlement Scheme Applications: Figures In Final Month, House of Commons Library, 14th June 2021, <https://commonslibrary.parliament.uk/eu-settlement-scheme-applications-figures-in-final-month/#:~:text=Although%20around%205.3%20million%20people,upper%20estimate%20of%204.1%20million>

198 Visas and Immigration, iProov, accessed 23rd March 2023, <https://www.iproov.com/what-we-do/use-cases/visas-and-immigration>

199 Unsettling – A Report On The Experience of EEA Nationals and Their Families In The EU Settlement Scheme, Migrant Voice, November 2021, <https://barrowcadbury.org.uk/wp-content/uploads/2019/11/Unsettling-Migrant-Voice-Settled-Status-Report.pdf>

200 Access Denied: The Case Against A Two-Tier Britain Under Covid Certification, Big Brother Watch, 2nd April 2021, <https://bigbrotherwatch.org.uk/wp-content/uploads/2021/04/Access-Denied-Big-Brother-Watch.pdf>

Right To Work

UK law requires employers to conduct a “Right to Work” check on all new employees, with fines being levied against companies that fail to verify this status. This can be done by checking copies of original documents, such as a passport and work visa, or by using a digital government service to generate a code which verifies a person’s right to work.

Although document checking sounds like a more analogue and old-fashioned way of verifying a person’s immigration status, several companies offer remote or digital document checks [rather than a share code] which compare photographs of a potential employee’s documentation against their face to verify their status.

Credit reference agency TransUnion is one of the many companies marketing virtual right-to-work checks. It claims that a mobile phone or computer camera can validate the veracity of a document, with employers also offering the option to ask candidates to take a selfie which is matched against the document using facial recognition. It appears to work similarly to the EUSS verification scheme. TransUnion promotes the tool as freeing up HR staff time and allowing companies to show that they are efficient.²⁰¹

Other companies offering similar services include Experian, another credit reference agency, data company Yoti which has partnered with the Post Office to build its tool, and specialised firms Sterling Check and Trust ID.²⁰² The proliferation of companies offering this solution suggests there is a rising use of facial recognition at the intersection of immigration and employment.

If potential employees are asked to do digital right-to-work checks, there must be an option for them to opt out of biometric processing. As physical document checks are accepted by the government, it is unlikely that processing biometric data can be regarded as necessary. Employers would therefore have to rely on consent as legal grounds for facial recognition – which should be freely given and alternative options presented to prospective new hires.

201 Document Verification and Facial Recognition, TransUnion, accessed 19th March 2023, <https://www.transunion.co.uk/content/dam/transunion/gb/business/products/resources/TruValidateDocument-Verification-Facial-Recognition-Right-to-work-asset.pdf>

202 Yoti, Post Office Digital ID Service First Certified By UK For Employee Vetting, Biometric Update, 6th June 2022, <https://www.biometricupdate.com/202206/yoti-post-office-digital-id-service-first-certified-by-uk-for-employee-vetting>

“We must continue to resist the use of this technology which has been proved to be biased against racially minoritised communities, particularly Black people”

- Dr Laura Loyola-Hernández, Yorkshire Resists

Commentary – Dr Laura Loyola-Hernández, Yorkshire Resists

“Racial and sexist bias in Facial Recognition Technology (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. This implies that Black people are more likely to be misidentified by police FRT and questioned on the basis of a false alert.

“Since December 2021, Operator Initiated Facial Recognition [OIFR], a mobile phone use of Facial Recognition Technology [FRT], has been piloted by South Wales Police and Gwent 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. The initial number of officers using this technology is 70. We at Yorkshire Resists and the Racial Justice Network submitted an FOI to South Wales and Gwent Police in relation to the force’s use of overt facial recognition technology in mobile devices, from December 2021 to March 2022. Our findings reflect concerns that this technology is primarily used on grounds of ‘suspicion’ and thus subject to misuse and racial profiling.²⁰³ The use of this technology is not limited to policing. FRT is being used more and more in our daily lives.

“In November 2021, the Independent Workers’ Union of Great Britain (IWGB) and the App Drivers and Couriers Union (ADCU) took legal action against Uber via an employment tribunal saying the facial recognition software used to verify their identity at the start of every shift discriminates against darker skin tones. This is just one example of employers using surveilling technology in the name of efficiency and to “comply” with legal requirements imposed by the UK’s hostile environment policies. Employers must check people have the right to work in the UK via right to work checks. Universities, companies, hospitals and many other employers are increasingly using third party apps, including facial recognition, to do these checks.

“These types of checks discriminate against migrants, particularly those from racially minoritised communities. Migrants’ Rights Network is leading the campaign to challenge these checks.²⁰⁴

“We are concerned by the way in which FRT is encroaching in our daily lives, in our

203 #HandsOffOurBiodata: Mobilising Against Police Use of Biometric Fingerprint and Facial Recognition Technology, Stop the Scan [Racial Justice Network and Yorkshire Resists], October 2022, <https://stopthescan438237173.files.wordpress.com/2022/10/final-sts-20-22-foi-report-2.pdf>

204 Challenge The Checks, Migrants Rights Network, accessed 12th April 2023, <https://migrantsrights.org.uk/projects/challenge-the-checks/>

workplaces and to surveil our communities. We must continue to resist the use of this technology which has been proved to be biased against racially minoritised communities, particularly Black people.

None of us are free until all of us are.”

Private Sector Facial Recognition



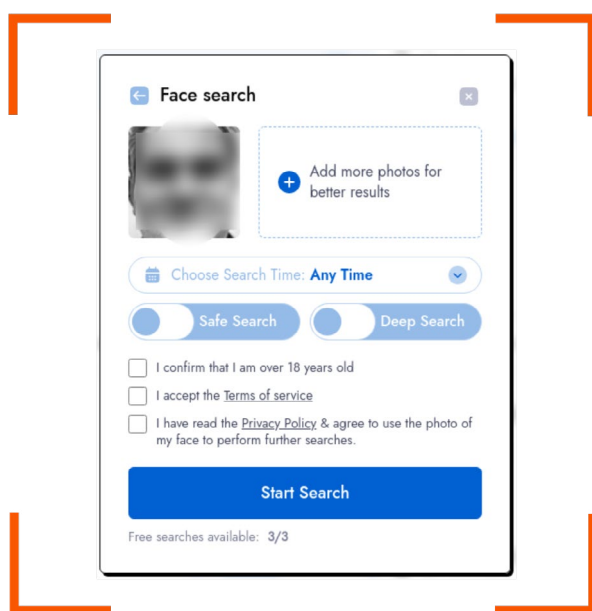
PimEyes

What Is PimEyes?

PimEyes describes itself as a “face search engine reverse image search”.²⁰⁵ It allows users to upload a photograph of a person and find any other images published of that person online, using facial recognition to identify relevant photographs from a database of at least 900 million images.

The company was founded by two graduates of the University of Science and Technology in Wrocław, Poland, Łukasz Kowalczyk and Denis Tatina.²⁰⁶ It is now owned by a Georgian academic, Giorgi Gobronidze, via a company registered in Dubai.²⁰⁷ However, the point of contact on the PimEyes website lists a company called Carribex in the Central American tax haven Belize, underlining the lack of transparency surrounding the firm.²⁰⁸

Anybody with an internet connection can use PimEyes and there are no checks to ensure that users are only searching for themselves or people who have consented to their images being used. The company claims that its terms restrict searches to users’ own faces, although its enforcement of this is limited to a box which the user must tick before searching.



PimEyes uses FRT to compare an uploaded photograph to all other images in the database. Those thought to be sufficiently similar are returned as results, alongside the source URL of the matched image.

Results are pulled from across the internet. Although social media platforms are not scraped, images are pulled from blogs, news articles, reviews and even pornography websites.²⁰⁹ Journalists from the New York Times ran their own photographs

205 PimEyes website, accessed 8th February 2023, <https://pimeyes.com/en>

206 A Polish Company is Abolishing Our Anonymity, [Netzpolitik.org](https://netzpolitik.org), 10th July 2020, Łukasz Kowalczyk and Denis Tatin, <https://netzpolitik.org/2020/pimeyes-face-search-company-is-abolishing-our-anonymity/>

207 A Face Search Engine Anyone Can Use Is Alarmingly Accurate, The New York Times, 29th May 2022, <https://www.nytimes.com/2022/05/26/technology/pimeyes-facial-recognition-search.html>

208 PimEyes Privacy Policy, accessed 22nd March 2023, <https://pimeyes.com/en/privacy-policy>

209 A Face Search Engine Anyone Can Use Is Alarmingly Accurate, The New York Times, 29th May 2022, <https://www.nytimes.com/2022/05/26/technology/pimeyes-facial-recognition-search.html>

through PimEyes and found that although most results were correct, there were some errors, most notably false matches for the women that were sourced from adult websites.

At different pricing points, PimEyes allows users to make frequent use of the tool. For around £30 per month, users can conduct 25 daily searches and set up 'alerts' for three different images [which PimEyes claims may be for different photos of oneself, rather than third parties]. At £40 per month, this rises to 15 alerts, with PimEyes also offering support to issue DMCA and GDPR takedown notices for images. At £300 per month, searches are unlimited, with 500 images for alerts and "deep search" which is marketed as a more thorough web scrape.

In addition to scraping the clearnet [ordinary internet] for most users, PimEyes also offers an advanced tool for law enforcement that focuses on child abuse material. The company provides its tool to Paliscope, a software package aimed at law enforcement, which in turn works with 4theOne Foundation which investigates child trafficking.

PimEyes offers an "opt-out" for people to use if they want to avoid their data being retrieved via facial recognition on their service. However, the opt-out does not stop a person's face from being searched, rather it restricts the return of search results above a certain similarity threshold when compared with the image submitted on the opt-out form. Such an opt-out also entails that the individual's sensitive personal data is retained and continually processed, in order to be continually discounted from search results that are returned. As such "opting out" of PimEyes' system means paying them to continually process sensitive biometric data that the individual did not allow them to process in the first place. Furthermore, the fact that the "opt out" service is central to PimEyes' business model demonstrates that the company is well aware that the product is designed to be used by third parties to search for an individual, rather than an individual to search for photos of themselves, as they market a product to prevent search results of an individual being returned in third parties' search results.

Traumatic Images

Software engineer Cher Scarlett, who has written about her experiences with PimEyes for this report, uncovered distressing images when she searched her face on the platform. The results included explicit images of her when she experienced sexual exploitation as a teenager, the memories of which she had repressed. She attempted to have her photos removed from PimEyes' search results, without success.²¹⁰ Many of the websites hosting the explicit photographs contained terms linked to violent sexual imagery, yet anyone searching with Ms Scarlett's face at the time would have found these images without her

210 She Thought A Dark Moment In Her Past Was Forgotten. Then She Scanned Her Face Online, CNN Business, 24th May 2022, <https://edition.cnn.com/2022/05/24/tech/cher-scarlett-facial-recognition-trauma/index.html>

knowledge.

As well as surfacing images linked to past traumas, Ms Scarlett found multiple images of dead relatives via PimEyes. The combination of the automated scraping of images and matching based on facial similarity means that people who resemble her, such as her deceased sister, were returned in the search results.²¹¹ They also included an image of her mother as a child [which came back when Ms Scarlett uploaded one of her own baby photos] and a monochrome photo of her great-great-great grandmother that was more than a century old.

These images were pulled from the genealogy service Ancestry and its sister service Find a Grave, which the family history websites claim breach its own terms and conditions. As Ms Scarlett told WIRED, the dead can neither consent nor opt out of PimEyes' biometric searches, and the linking of deceased relatives to living people raises profound privacy and ethical issues. PimEyes has since claimed that its crawlers went awry and that they only search sites they are allowed to, and that it is now blocking Ancestry's domain and indexes related to it are being erased. However, if it has happened once, it suggests there is a risk of similar sites being crawled again without permission.²¹²

Data protection laws do not generally apply to the deceased, however it does not mean their data can be used without constraint. The European Court of Human Rights has found that if information relating to someone who has passed is used in a way that impacts somebody who is still alive, then data rights can be breached.²¹³ There is a risk that PimEyes could draw a connection between a person and their late relative in such a way as to have a detrimental impact on them and breach the living person's data rights.

Likewise, it is possible for living relatives, particularly those who look alike, to be matched without their knowledge or consent via a PimEyes search conducted by another member of their family on their own face. There is a significant privacy risk posed by incorrect matches, as a familial relationship does not entitle a person to have someone else's biometric data processed.

211 A Face Recognition Site Crawled the Web for Dead People's Photos, WIRED, 13th March 2023, <https://www.wired.co.uk/article/pimeyes-face-recognition-site-crawled-the-web-for-dead-peoples-photos>

212 A Face Recognition Site Crawled the Web for Dead People's Photos, WIRED, 13th March 2023, <https://www.wired.co.uk/article/pimeyes-face-recognition-site-crawled-the-web-for-dead-peoples-photos>

213 M.L v. Slovakia, 34159/7, European Court of Human Rights, 14th October 2021, <https://hudoc.echr.coe.int/fre?i=001-212150>

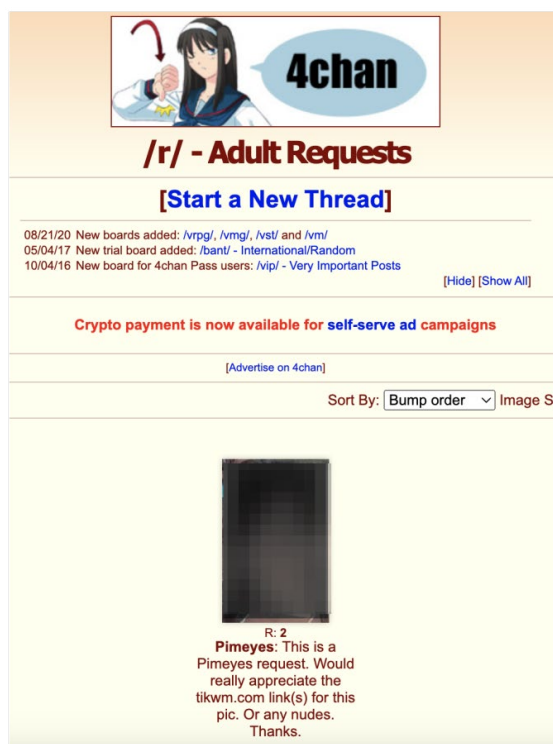
Cyberstalking

PimEyes also operates a referral or affiliate program where anyone can promote the tool and get paid up to \$75 [£62] for each person who signs up with their link. The company places no restrictions on how its affiliates promote and there is significant evidence that some of these affiliates breach PimEyes' terms when marketing the product.

In one example, uncovered by The Byline Times, an American YouTuber "The Skip Tracer" blatantly ignores PimEyes' restriction on only searching one's own face or consented-to images in a video "Karen Gets a Facial Recognition – SHOCKING Results!", which contains a link to his PimEyes affiliate link in the description.²¹⁴ He runs a face captured in a video posted by another YouTuber, "NastyNathanial", through the system. There is no way for the woman who appeared in the original videos to know that she had further been searched via PimEyes, her biometric data processed and her identity put at risk.²¹⁵

The PimEyes search returns several results for the unnamed woman, and the YouTube video focuses on a subset of those that appear to be adult images or videos. "The Skip Tracer" attempts to justify the search of the woman's face because she was filmed in public and because she took issue with "NastyNathanial" filming her in a public place. He claims that despite finding a "good amount of information" on her and implying this included her address, he would not share that on his YouTube channel.

A number of the comments underneath the video, including some "The Skip Tracer" responded to, made comments about the woman's adult entertainment work. The pinned comment [which is decided by the channel's owner] even features the woman's name, which the "Skip Tracer" claimed he did not want to share.



214 YouTube link not cited to protect the victim's privacy, but it is available on request

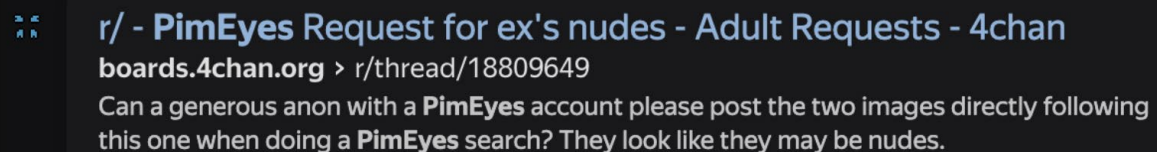
215 AI Search Engine PimEyes Facilitates Image-Based Sexual Abuse of Women...Then Sells Them the Solution, Byline Supplement, 17th April 2023, <https://www.bylinesupplement.com/p/ai-search-engine-pi-meyes-facilitates>

The same YouTuber repeatedly uses PimEyes in a number of his videos to track down and identify people he is looking at, underlining that how even repeated breaches of the company's terms [searching other people's faces] apparently lead to no action from PimEyes.

"The Skip Tracer" example also undermines PimEyes' claims in its privacy policy that it does not establish identity or hold personal data about individuals. At the very least it signposts strongly to information that will identify the subject of an image.

On 4Chan, the anonymous image board website, there are further examples of users sharing photos of women they may know and asking others to search their faces on PimEyes. Some of these requests are explicitly for nude photographs of their ex partners, or random women on the internet, and many were on a thread dedicated to "Adult Requests".

A brief internet search brings up countless examples of internet stalkers attempting to find photographs, including adult images shared without consent, almost exclusively of women. Some of the posts have been removed from 4Chan but evidence remains in the snippets saved in web searches.

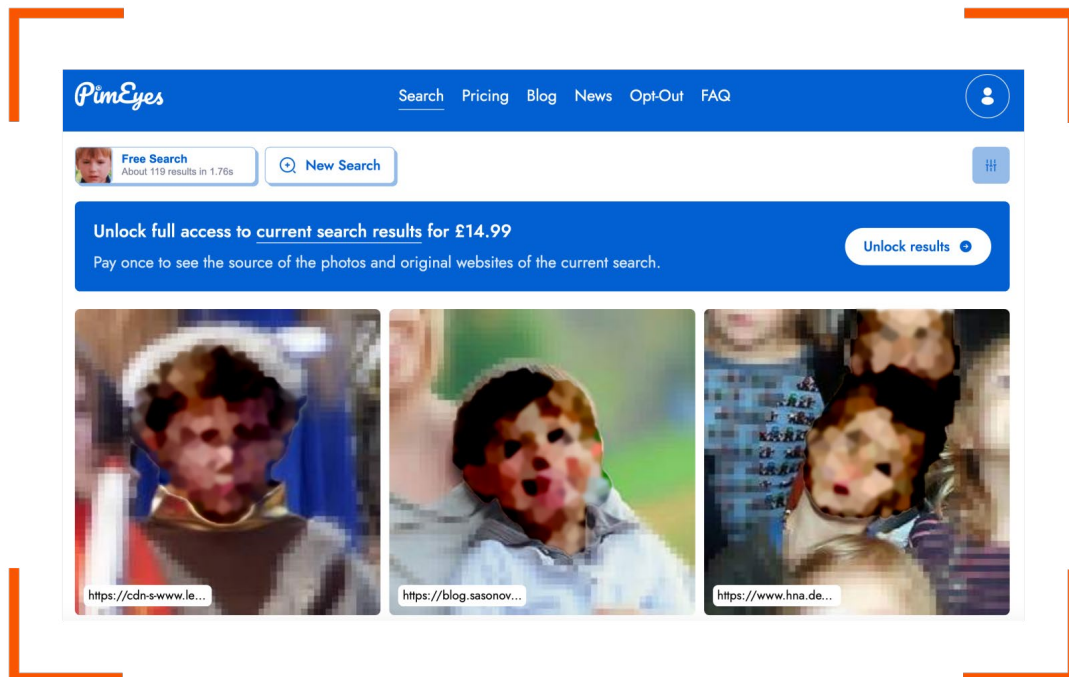


r/ - PimEyes Request for ex's nudes - Adult Requests - 4chan
boards.4chan.org > r/thread/18809649
Can a generous anon with a PimEyes account please post the two images directly following this one when doing a PimEyes search? They look like they may be nudes.

Big Brother Watch has not linked to any of the posts in the citations as to not further share links to potential abuse, but the above screenshots outline how commonplace it is for cyberstalkers to use PimEyes to target women online.

Children

Images of children can be searched on PimEyes, despite the website asking if a user is 18 before they conduct a search.



A member of the Big Brother Watch team tested the potential for PimEyes to search for photos of children by uploading a photograph of himself as a toddler, from the 1990s. The results were a number of photos of other children of a similar age and none of him, which was not surprising as there are few to no other photos of him as a young child online.

However, the result is that dozens, or more, children had their biometric data processed by PimEyes to return the potential matches for the search. These children have clearly not consented to biometric processing yet they are subjected to it by PimEyes. A child would be breaking PimEyes's terms if they searched their own photo – raising the question about how children can object to processing. Data protection law provides added protection to children's data rights – exacerbating the harm done by the non-consensual processing of their special category data.²¹⁶

Given the evidenced examples of PimEyes being used to non-consensually identify adult actors, or revenge porn, there is risk that explicit images of children could be returned as results or even sought out via a PimEyes search.

User Suggestions

Users can also post on a forum with ideas for PimEyes developers on how to upgrade or improve the service. One suggestion, which is in review and has many upvotes, was to allow users to specify which sites they wanted to find images on.²¹⁷ Several supporters of the post proceeded to name adult websites as examples of sites they wish to search

²¹⁶ Children, Key Data Protection Themes, Information Commissioner's Office, accessed 25th April 2023, <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/#:~:text=Children%20have%20the%20same%20rights,have%20their%20personal%20data%20erased.>

²¹⁷ PimEyes Suggestion, accessed 3rd April 2023, <https://pimeyes.kampsite.co/suggestions/ac70a8cc-7633-4972-9f10-49f89498a514>

specifically. Although PimEyes eventually clarified it does not scrape certain sites due to its “no-harm policy” its users’ intentions are clear.

Big Brother Watch Complaint

In November 2022, Big Brother Watch made formal submissions to the ICO alleging that PimEyes is in breach of Article 9 of the UK GDPR, which outlines individuals’ rights concerning special category data – of which biometric data [such as a faceprint] is one variety.²¹⁸

We explained that PimEyes processes the biometric data of millions of people in the UK, without a valid exemption as required under Article 9 of GDPR, such as consent. Furthermore, the checks to ensure that someone can only search for their own images are incredibly weak. There is also no notification of processing given to the data subject whose image is used, meaning that a person’s biometric and personal data may be processed without their knowledge or consent. We laid out many privacy threats posed by PimEyes, such as:

- A PimEyes user could track down large quantities of personal information about someone they know and have an image of
- A user could identify currently unknown people featured in images

Some of these threats particularly impact women and girls:

- PimEyes could be used to track down someone ahead of contacting them against their will or harassing them
- It could be used to uncover “revenge porn” posted of an individual known to a user – there is already evidence of PimEyes finding non-consensual explicit images
- Conversely, it could be used to track down someone seen in “revenge porn” or even child sexual abuse material used by a user as a probe image

PimEyes claims to not process personal data, stating that it instead indexes publicly available pictures online and points to where they might be found on the internet, rather than identifying them explicitly. Big Brother Watch believes that this is an incorrect understanding of GDPR as guidelines from the European Data Protection Board state that processing can make someone identifiable without directly linking to their identity for example “if the comparison is made against a database of photographs associated with a surname and a first name”.²¹⁹ On PimEyes many of the resulting images are clearly linked

²¹⁸ Big Brother Watch Submission to the Information Commissioner on PimEyes, November 2022

²¹⁹ Guidelines 05/2022 On The Use Of Facial Recognition Technology in Law Enforcement, European Data Protection Board, 12th May 2022, https://edpb.europa.eu/system/files/2022-05/edpb-guide-lines_202205_frtlawenforcement_en_1.pdf

to individuals' names.

Among the other alleged breaches of the GDPR, Big Brother Watch also pointed out that PimEyes currently has no UK representative as is required by Article 27 of the UK GDPR, meaning that despite potentially processing millions of UK residents' personal data there is no local point of contact in the UK.

On 13th April 2023 the Information Commissioner's Office contacted Big Brother Watch to say it would take no further action against PimEyes. No explanation was given, nor was any comment on PimEyes' data protection compliance.

Clearview AI

Clearview is a US-based facial recognition company which offers a “face search” capability for uploaded images against its database of more than 30 billion facial images.^{220,221} The service is marketed at law enforcement but in the past, it has offered its facial recognition to commercial companies and even universities. Clients have been known to include a number of UK police forces, the FBI, and the US Department of Homeland Security. The images in Clearview’s 30 billion-strong database are indexed from all around the web, including social media sites.

Australian entrepreneur Hoan Ton-That is the CEO of Clearview AI, co-founding the company with the Republican politician Richard Schwartz.

The company was initially known as Smartcheckr and was registered in New York in 2019, with Clearview being registered in Delaware later in 2019. In its early days, there were allegations that Clearview had made misleading marketing claims, attempting to take responsibility for the identification and arrests of people wanted for an assault and a sexual assault in New York. However, the NYPD later said Clearview played no role in either case.²²²

How It Works

Clearview’s facial recognition works functionally like police retrospective facial recognition systems, or PimEyes. It is a facial recognition search engine that compares a probe image to the images held on its massive database and then returns any results deemed to be a match. Any potential matches are returned alongside the image’s original URL.²²³

What differentiates Clearview from police systems, and even PimEyes, is the indiscriminate web scraping it uses to collect images and the subsequent scale of its database. Police RFR relies mostly on custody images, while PimEyes claims its own web crawlers are limited and do not cover social media websites. PimEyes’ database is around 1/30th of the size of Clearview’s.

220 Clearview AI Settles Suit And Agrees To Limit Sales Of Facial Recognition Database, The New York Times, 9th May 2022, <https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html>

221 Clearview AI Used Nearly 1m Times By US Police, BBC News, 27th March 2023, <https://www.bbc.co.uk/news/technology-65057011>

222 Clearview AI Says Its Facial Recognition Software Identified A Terrorism Suspect. The Cops Say That’s Not True, BuzzFeed News, 23rd January 2020, <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-nypd-facial-recognition>

223 Law Enforcement, Clearview AI, accessed 30th March 2023, <https://www.clearview.ai/law-enforcement>

Who Uses It

The facial recognition tool is aimed at law enforcement and arms of government, with the company claiming state bodies are presently its only customers.²²⁴ Clearview claims it has run nearly one million facial searches for police forces in the United States of America alone.²²⁵ A number of UK police forces reportedly used the software before the Information Commissioner banned it in the UK. This included North Yorkshire Police, Northamptonshire Police, the Metropolitan Police, Surrey Police, North Yorkshire Police, Suffolk Constabulary and the National Crime Agency.²²⁶

Documents seen by BuzzFeed News indicated that the NCA had used Clearview at least 500 times while the Met Police had conducted more than 170 searches on Clearview and Northamptonshire Police had run more than 160. According to the documents, accounts associated with the Ministry of Defence as well as financial services companies and even J.K. Rowling's charity Lumos had accounts with Clearview, which may have been used for demonstration purposes.²²⁷

Aside from police forces in the US, Clearview has previously been used by some private sector organisations, such as supermarket chain Walmart, department store Macy's and the National Basketball Association.²²⁸

ICO Ban in the UK

In May 2022, the Information Commissioner's Office fined Clearview AI more than £7.5 million, ordering the company to stop collecting the data of UK citizens and delete any it continued to hold.²²⁹

The ICO, which conducted a joint investigation with the Office of the Australian Information Commissioner [OAIC], found that Clearview's non-consensual scraping of millions of UK residents' photos violated data protection laws in several ways. This included handling personal data in a non-transparent way, as people would not have expected their photos to be scraped, failing to have a lawful reason for collecting the data and not meeting the

224 Principles, Clearview AI, accessed 30th March 2023, <https://www.clearview.ai/principles>

225 Clearview AI Used Nearly 1 Million Times By US Police, It Tells The BBC, BBC News, 28th March 2023, <https://www.bbc.co.uk/news/technology-65057011>

226 More Than A Dozen Organizations From The Met Police To J.K. Rowling's Foundation Have Tried Clearview AI's Facial Recognition Tech, BuzzFeed News, 28th February 2020, <https://www.buzzfeed.com/emilyashton/clearview-users-police-uk>

227 Ibid

228 Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA, BuzzFeed News, 27th February 2020, <https://www.buzzfeednews.com/article/ryan-mac/clearview-ai-fbi-ice-global-law-enforcement>

229 ICO Fines Facial Recognition Database Company Clearview AI Inc More Than £7.5m and Orders UK Data To Be Deleted, ICO, 23rd May 2022, <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/>

data protection standards for handling biometrics.²³⁰

By the time the ICO/OAIC investigation had concluded Clearview had stopped offering its products to organisations in the UK. However, the ICO still issued an enforcement notice, ordering the company to halt obtaining UK data and delete any it held as the nature of Clearview's indiscriminate web-scraping means that a large number of UK residents' photos would still be held.²³¹

It is highly unlikely and technically unfeasible that Clearview has complied with the order to stop collecting data from the UK and delete any UK residents' data that it still holds, given the technical challenges that identifying all the relevant images would entail. Individuals can ask Clearview to delete data held on them, but this requires an identifying photo to be used as a probe image – a practice that was condemned by the ICO in its ruling.

Across Europe, data protection regulators have issued other fines after finding that Clearview's activities broke data protection law. The Commission Nationale De L'informatique Et Des Libertés [CNIL], the French data regulator, issued the company with a €20 million fine in October 2022, as did the Italian and Greek privacy watchdogs.²³² In the United States, the company has been forced to limit its activities following a legal case in Illinois, which led to Clearview agreeing to only market its products to law enforcement and other government agencies.²³³

Policy Analysis

Online facial recognition tools, such as Clearview AI and PimEyes, incur invasions of privacy on a previously unimaginable scale. Facial recognition search engines curate and biometrically scan databases made up of billions of photos, without the knowledge or permission of individuals whose faces are on there. Whether used by police forces, government bodies or private individuals, these tools result in a major breach of privacy rights on a mass scale, not to mention endangering individual safety. The use of facial recognition to identify people among potentially billions of photos threatens to end anonymity as we know it. Anyone who has ever appeared in a photo on the internet could be part of a facial recognition database, incurring a risk of both being identified and tracked online, but also of having their sensitive data unlawfully processed every time a facial recognition search is conducted.

230 Ibid

231 Clearview AI Enforcement Notice, Information Commissioner, 18th May 2022, <https://ico.org.uk/media/action-weve-taken/enforcement-notices/4020437/clearview-ai-inc-en-20220518.pdf>

232 France Fines Clearview Ai Maximum Possible For Gdpr Breaches, TechCrunch, 20th October 2022, <https://techcrunch.com/2022/10/20/clearview-ai-fined-in-france/>

233 Clearview Ai Settles Suit And Agrees To Limit Sales Of Facial Recognition Database, New York Times, 9th May 2022, <https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html>

Clearview and PimEyes process the sensitive biometric data of UK residents. This mass processing has no lawful basis under data protection law. The ICO's decision to fine Clearview AI £7.5 million, as well as ordering the company "to stop obtaining and using the personal data of UK residents that is publicly available on the internet, and to delete the data of UK residents from its systems" was a welcome intervention, and confirmed that these tools pose a serious risk to privacy and data rights.²³⁴ The decision, then, of the ICO not to take regulatory action against PimEyes, in response to Big Brother Watch's complaint appears inexplicable and is deeply concerning. The Baden-Württemberg data protection authority in Germany has initiated legal proceedings against PimEyes, citing concerns over the company's processing of biometric data, the lack of consent from data subjects, an opt-out option that places the onus on the data subject to protect their data from being made accessible to an indefinite number of people, and the possibility of third party abuse.²³⁵ These mass facial recognition search engines are not compatible with data protection law, and the ICO must prohibit them from operating in the UK and processing the biometric data of people in the UK without consent.

As well as unlawfully processing the biometric data of UK citizens, PimEyes poses a significant risk to the privacy and safety of individuals. The tool's total absence of safeguards mean it could be secretly used by potential employers, university admissions officers, domestic abusers or stalkers. Photos from media articles, personal blogs, dating websites, employment profiles, and other publicly available websites can all be surfaced. Given that the returned facial images are provided alongside the URLs where they are hosted, highly revealing contextual information about the searched individual is likely to be uncovered. This could include their name, details about their place of work, or indications of the area in which they live. It is also possible that information about an individual's religious or political views, their sexuality or gender identity could be revealed.

The potential negative outcomes for individuals are serious and could put people at risk of harm. The considerable evidence above suggesting that these tools are being used to identify and track women who appear, either consensually or non-consensually, in sexually explicit content online, is deeply chilling. Online facial recognition is putting women at serious risk. Widespread and unfettered use of these tools is already leading to a new era of technology-powered sexual harassment, threats and stalking. The ICO must urgently step in to safeguard UK residents from such abuses.

234 ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted – Information Commissioner's Office, 23rd May 2022, <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/>

235 PimEyes: LfDI opens fine proceedings, LfDI Baden-Württemberg, 21st December 2022 (translated from German), <https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/>

“When the results from the PimEyes search came back, with images of a sexual trauma I had repressed, I was overcome with grief and agony.”

- Cher Scarlett

Commentary From Cher Scarlett

"As a survivor of commercial sexual exploitation, revenge porn, and doxxing on websites like 4chan, I understand first-hand how crucial ethical boundaries are in technology to prevent harm. PimEyes' facial recognition tool allows predators to access victims like me without our consent. Despite opting out, I'm still enrolled in their database. It is essential for companies like PimEyes to be held accountable for their actions and for regulations to be in place to prevent further harm to vulnerable groups.

"Last year, a tweet about facial recognition software's potential for use in persecution and potentially genocide led a journalist to reach out to about PimEyes. I was researching how this technology poses a risk to ethnic minorities, as I am descended from Volga Germans who were deported to Siberia under Stalin, and saw mirrors in Chinese tech companies' creation of "Uyghur Alert" systems. I tried PimEyes, which has scraped the web for billions of faces and created a facial geometry search database without our knowledge or consent.

"When the results from the PimEyes search came back, with images of a sexual trauma I had repressed, I was overcome with grief and agony. I had blocked out what happened to me as a teenager and here it was, two decades later, on the internet for anyone to find. I paid the \$300 for the deep search tier to hide it. They refunded me and directed me to opt-out, but it didn't work. Months went by and you could still find it, much to the joy of internet trolls.

"When Big Brother Watch filed an ICO complaint in the UK, I was inspired to dig into US law. I found an avenue for action in Washington State law and filed a complaint on 6th January 2023. After receiving it on 18th January, PimEyes hid me from their search results and banned my account. They claimed that they had removed my photos when I opted out. However, on 13th January, I tweeted real-time screenshots proving the opt-out did not work. I suspect PimEyes traced my IP address and manually hid results from my own search history. I deleted my account and remade it without needing to verify my email address—all of my prior account history was accessible.

"Although PimEyes now hides my commercial sexual exploitation results, I remain enrolled in their database and I cannot effectively opt-out. My photos are still re-indexed when their crawlers find a new photo, leaving me and other victims of exploitation vulnerable to further searching and distribution.

This software should be shut down immediately."

Facewatch

Facewatch is a British company, founded by Simon Gordon of Gordon's Wine Bar in central London, which offers live facial recognition to businesses in the UK and abroad. It claims that the system can "reduce store theft" and create a "safer" retail environment.²³⁶ The company aims to "commoditise" facial recognition so even corner shops can afford it, creating a mass surveillance network in the process.²³⁷

Many well-known retailers and businesses are among Facewatch's clients. They include:

- 35 Southern Co-Op stores across London and the South of England
- At least 27 shops owned by Mike Ashley's Frasers Group that Big Brother Watch has identified, including:
 - 13 Flannels department stores
 - 12 Sports Direct shops
 - 2 USC outlets
- Luton Town Football Club
- SPAR shops
- Budgens convenience stores
- Costcutter convenience stores
- Quality Discounts [QD] discount retailers
- Whitehall Garden Centres
- Tian Tian Market [an Asian supermarket]
- Village Wholefoods

As well as its UK operations Facewatch has distributors in Spain, Brazil and Argentina.²³⁸ The company deployed its facial recognition technology as far back as 2017 in a Rio de Janeiro shopping centre.²³⁹

Founded in 2010, Facewatch was originally a crime reporting and intelligence-sharing tool for businesses, business improvement districts [BIDs] and the police. The original iteration of the product allowed for the rapid sharing of CCTV images of suspected crimes among this group, including facial images, and the company worked closely with police forces.²⁴⁰ In 2012, it was reported that Facewatch would allow the general public to search through almost 5,000 images of wanted individuals and send a name to the police via the platform if they recognised anybody.²⁴¹

236 Facewatch website, accessed 22nd March 2023, <https://www.facewatch.co.uk/>, <https://www.buzz-feed.com/emilyashton/clearview-users-police-uk>

237 Facewatch And Vista Cctv, Introducing The New Distribution Partnership, Facewatch, Youtube, 5th March 2020

238 Facewatch: The Reality Behind The Marketing Discourse, Privacy International, 15th October 2020, https://www.youtube.com/watch?v=XjM_8RV1EDY&t=3s <https://privacyinternational.org/long-read/4216/facewatch-reality-behind-marketing-discourse>

239 Facewatch in Brazil, Professional Security Magazine, 4th October 2017, <https://www.professionalsecurity.co.uk/news/commercial-security/facewatch-in-brazil/>

240 Facewatch Pilot Combats Retail Crime In 2021, City Security, 4th July 2018, <https://citysecuritymagazine.com/police-partnerships/facewatch-pilot-combats-retail-crime-in-2012/>

241 'Facewatch' App Allows Citizens In UK To ID Suspects, Police1, 26th June 2012. <https://www.police1>

It appears that Facewatch pivoted from being primarily an intelligence-sharing platform to a facial recognition system in early 2018 with Internet Archive evidence showing that the company's website was revamped and began to focus on FRT at that time.

In addition to Big Brother Watch's complaint about the company's data processing, Facewatch was independently investigated by the Information Commissioner. It was required to make major changes due to the ICO identifying areas of concern with how it handled personal data, though neither the ICO nor Facewatch has disclosed exactly what those changes were.^{242,243,244} Despite this, Facewatch has always asserted that its system is compliant with GDPR protections and has posted on its social media channels that the ICO "cleared the way" for Facewatch.²⁴⁵

How Does It Work?

As with police-operated live facial recognition, Facewatch operates via software that monitors live video feeds from the entrance of a premise to detect any faces walking through a camera's field of vision. These faces converted into biometric templates and compared against the biometric templates stored on the Facewatch watchlist. If the system finds a match that is above the pre-set threshold of similarity [communicated as a percentage score] it then sends an alert to shop staff to act in line with the retailers' policy.²⁴⁶

Facewatch is designed as a software tool which can plug into almost any brand of HD CCTV camera, which is one of the key reasons it threatens to roll out a huge network of privatised facial recognition nationwide. In March 2023 the company said it was no longer using cameras from Hikvision, the Chinese state-owned company linked to genocide in Xinjiang, a sharp U-turn from Nick Fisher's advocacy of Hikvision. In 2020 he said "I know Hikvision well, great quality products at affordable prices" when talking to a Facewatch installer on a YouTube video.^{247,248}

[com/police-products/police-technology/articles/facewatch-app-allows-citizens-in-uk-to-id-suspects-gU4IRsJ2YhS3oox7/](https://ico.org.uk/about-the-ico/media-centre/blog-balancing-people-s-privacy-rights-with-the-need-to-prevent-crime/)

242 Blog: Balancing People's Privacy Rights With The Need To Prevent Crime, Information Commissioner's Office, 31st March 2023, <https://ico.org.uk/about-the-ico/media-centre/blog-balancing-people-s-privacy-rights-with-the-need-to-prevent-crime/>

243 Freedom of Information Request to the ICO, IC-199200-W8C8, 16th November 2022

244 Freedom of Information Request to the ICO, IC-165465-D8B0, 26th April 2022

245 Facewatch, LinkedIn, April 2023, https://www.linkedin.com/posts/facewatch_breaking-news-ico-judgement-clears-activity-7047498603514200065-k_Z?utm_source=share&utm_medium=member_desktop

246 Facewatch Installer Guide, accessed 22nd March 2023, <https://www.facewatch.co.uk/wp-content/uploads/2020/03/Facewatch-Installer-Guide-v2f-web.pdf>

247 FACE2FACE with Nick Fisher, CEO, Facewatch and Gavin Dunleavy, Commercial Director, DVS Ltd, Facewatch, Youtube, 17th January 2020, <https://www.youtube.com/watch?v=UKIRv6OVyR8>

248 Facewatch To Stop Using Hikvision Amid Controversy Over Uk Retail Biometrics, Biometric Update, 23rd March 2023, <https://www.biometricupdate.com/202303/facewatch-to-stop-using-hikvision-amid-controversy-over-uk-retail-biometrics>

The Watchlist

Facewatch maintains a master database, dubbed the “National Watchlist”, which is made up of all the Subjects of Interest [SOIs] it holds information on. Although this language mirrors law enforcement terminology for suspects, it is not akin to a police “subject of interest” in a criminal investigation.²⁴⁹

This “National Watchlist” is created from the uploads of images and reports of incidents of crime and disorder from its subscribers across the country. These reports include the date of the alleged incident, a photo of the SOI and their name if known, and a summary of the incident. Facewatch documentation also states that it adds potential SOIs whose images are shared by either police forces or Crimestoppers to its database.

Subscribers [such as branches of the Southern Co-op] appoint staff members to upload incident reports, which can be backdated by up to two years. Although Facewatch markets itself primarily as an anti-theft and anti-abuse tool, the categories of the incident available for subscribers to upload information on have a wide scope, they include:²⁵⁰

- Theft, e.g – shop theft, till snatch, making off without paying, robbery
- Damage, e.g – damage to property, graffiti, vandalism
- Abuse, e.g – physical abuse, public order, verbal abuse
- Fraud, e.g – credit card fraud, counterfeit currency, cheque fraud
- Urban explorer²⁵¹
- Anti-social behaviour, e.g – begging, drugs, empty packaging, street drinking, vagrancy

The last set of incidents underlines how Facewatch has the potential to become a tool for socio-economic discrimination to eliminate so-called “undesirables” from the public sphere. Street drinking and being homeless [vagrancy] are not necessarily even offences, but to include these as potential watchlist incidents suggest that preventing crime is not the company’s only aim.

Video marketing materials published by the company also betray the potential wider social conditioning uses for Facewatch, with its product development manager discussing “undesirables” and people who are “generally causing trouble” on YouTube.²⁵² He adds that a key aim is to discourage these individuals from entering a store.

249 Subject of Interest Detailed Privacy Notice (‘SOI Notice’), Facewatch, accessed 22nd March 2023, <https://www.facewatch.co.uk/wp-content/uploads/2018/09/Subjects-of-Interest-Detailed-Privacy-notice.pdf>,

250 Facewatch User Guide, accessed 22nd March 2023, <https://www.facewatch.co.uk/wp-content/uploads/2020/04/User-Guide-V1.1-web.pdf>

251 George’s Tech Tips – Vlog #1 Introduction, Facewatch, YouTube, 11th May 2020, https://www.youtube.com/watch?v=jic-114_bil

252 George’s Tech Tips – Vlog #1 Introduction, Facewatch, YouTube, 11th May 2020, https://www.youtube.com/watch?v=jic-114_bil

Facewatch claims that its terms and conditions prohibit false incident reports and in its user guide subscribers do have to confirm they believe that the report to be true before adding them to the system. Its privacy policy also states that its staff check that there are “reasonable grounds to suspect that an individual is responsible for an act of crime”, however no detail of the standard of proof required to justify inclusion is given, leaving unanswered questions about the evidence needed to put somebody in a list.²⁵³

Each store subscribed has a tailored version of Facewatch’s National Watchlist, which is based on what the company believes is “adequate, relevant and necessary”. Although it is not clear what it deems to be necessary Facewatch has some sharing guidelines, which depend on the location of a subscriber’s premises. The radius within which a SOI generates an alert varies from eight miles in London to 15 miles in other cities, 26 miles in semi-rural locations and 43 miles in very rural areas.²⁵⁴

Unlike “traditional” blacklists held by shops, which usually took the form of a handful of photos of known local offenders stuck up in the back office [the data rights implications of which are not discussed here], this could potentially lead to someone triggering an alert and being challenged in a shop they have never been in before. The scope for surveillance with Facewatch is orders of magnitude larger than isolated shop blacklists.

The company claims that it is the legal data controller for the watchlists and that it takes on the data protection risk, while subscribers are data processors.²⁵⁵ This is a claim Big Brother Watch has disputed in its complaint to the Information Commissioner about the use of facial recognition in Southern Co-op shops. Subscribers have significant influence over the watchlist makeup [via incident reports], how the watchlist information is used in terms of acting on alerts and making the decision to deploy LFR. All of this means that both Facewatch and its clients are mutually involved in the data processing and are likely to be joint controllers.

Facial Matching & Alerts

Facewatch’s software detects and analyses the faces of anybody walking through the camera’s field of view. The facial recognition algorithms then compare the face to those on that store’s watchlist and if there are any matches, an alert is generated and sent to staff mobile devices. Shop staff can either verify the alert as a match or reject it. If an alert is ignored it is deleted after an hour.²⁵⁶ What happens when a match is confirmed is up

253 Facewatch Privacy Notice, accessed 22nd March 2022, https://www.facewatch.co.uk/privacy/?gl=1*1hdpd9j*_ga*MTE5MTYyMzAyMy4xNjc5NTAzNzE4*_up*MQ.

254 Facewatch User Guide, accessed 22nd March 2023, <https://www.facewatch.co.uk/wp-content/uploads/2020/04/User-Guide-V1.1-web.pdf>

255 Facewatch Overview, accessed 23rd March 2023, https://www.facewatch.co.uk/wp-content/uploads/2020/03/Facewatch-Single_page_fact_sheet-v1b.pdf

256 Facewatch User Guide, accessed 22nd March 2023, <https://www.facewatch.co.uk/wp-content/uploads/2020/04/User-Guide-V1.1-web.pdf>

to the individual shop, but it could range from a reminder that staff are present, to being asked to leave the premises.

The company also claims that all its alerts are double-checked by a secondary facial recognition algorithm, run by Amazon Web Services, and that alerts are only sent if “there is at least a 98 per cent similarity”.²⁵⁷

Non-Retail Uses

A since-deleted sample Information Sharing Agreement [ISA] posted online by Facewatch shows that the company had looked to work with the police to allow law enforcement to tap into the facial recognition system.²⁵⁸ Although there is no evidence that these agreements were ever implemented it shines a light on how privatised facial recognition could be expanded and become a network of police surveillance.

The ISA outlined that the police could be provided with four categories of alerts:

- Low risk – who are reasonably suspected of a crime and pose no undue risk to the public if challenged, if they are seen by the system a “just seen” alert is sent to the police. It is vague as to whether businesses would also receive an alert about this person but it appears they may do, this would include names.
 - Crime examples include Shoplifting, Employee Theft, Pick-pocketing or theft from a person, Deception & Fraud, Public nuisance, Public order offences, Serious acquisitive crime, Alcohol-related offences, Drug-related offences, Robbery, Burglary, Cybercriminals
- Medium/High Risk – Police can upload images related to convicts/suspects of major crimes, or people who pose an undue risk to the public if challenged. Facewatch alerts in this case are sent only to the police and are held on a segregated system.
 - Crime examples include violent criminals not considered appropriate for sharing as low risk, racially aggravated offences, violence or threat of violence, use or threat of weapons, paedophiles
- Highest Risk – no detail is given about this category, but it is described as a police-only segregated system where the watchlist is generated by police alone.

²⁵⁷ Privacy Policy. Facewatch, accessed 4th April 2023, <https://www.facewatch.co.uk/privacy/#mop>

²⁵⁸ Purpose Specific Information Sharing Agreement (“ISA”) Between Police And Facewatch, 4th September 2019

- Missing persons - Police can upload missing person's images to a watchlist for police-only alerts to be generated if they are sighted

Nick Fisher, Facewatch CEO, has also boasted of the system being trialled in the prison system and at football clubs but little further detail on this is available publicly.²⁵⁹

Policy Analysis

The use of live facial recognition in retail environments is a deeply concerning development that highlights the Government's failure to regulate the use of new forms of biometric surveillance. LFR is a highly intrusive form of surveillance that can monitor and identify individuals in real-time without their knowledge or consent. Using this technology to scan shoppers is disproportionate and unnecessary, and the consequences of being misidentified or wrongly placed on a watchlist could be serious. Members of the public could be prevented from making essential purchases, including food, be subject to intrusive interventions, or be brought into dangerous confrontations with security staff. All of these things could happen even when an individual has never committed an offence. Given that interventions happen in public, the repercussions for an individual's life, employment and social relationships could be catastrophic.



The use of LFR in retail environments means that all shoppers are subject to intrusive facial scans, where they are compared against a privately held watchlist. Many individuals,

²⁵⁹ Facial Recognition: Fiona Barton QC and Facewatch Present, Facewatch, YouTube, 17th February 2020, <https://www.youtube.com/watch?v=Wm77yHGFAUc>

when we visited a Southern Co-op store to speak to the public about the technology, were unaware LFR was even being used and that their faces had just been scanned.²⁶⁰ Many stickers warning members of the public that the technology is being used in stores are small and placed in locations that are easily missed.

The mass processing of such sensitive personal data must have a legitimate purpose under the GDPR and meet a high threshold of necessity and proportionality. As set out in our legal complaint to the ICO, we do not believe Facewatch has met these legal standards.²⁶¹ The ICO's decision to not meaningfully engage with our concerns through their investigation into Facewatch's technology is deeply concerning, completely out of step with other European data authorities [see, for example, Mercadona case, AEPD (Spain), PS/00120/2021 and the actions of the Dutch data protection authority in 2020] and leaves the door open for the biometric surveillance of shoppers in the UK on a vast scale.^{262,263,264}

This use of LFR creates new zones of privatised policing. Criminal offences such as harassment, violence towards staff or shoplifting should be handled by police officers, rather than by private facial recognition companies. If an individual is suspected of breaking the law, they should be subject to the criminal justice system, where they will have the chance to face charges and respond. This punitive business-led policing cannot be considered a fair and just alternative. There is no oversight as to who is placed on a watchlist, and individuals placed on a watchlist have no clear mechanism to challenge accusations made against them. Vulnerable individuals, such as young people or people with mental health problems, are particularly at risk of being barred from their local shops and potentially struggling to clear their name. Security guards and trained staff members are far better equipped to oversee who is permitted to enter a store. A surveillance system that automatically bars certain individuals risks automating discriminatory, unfair or inaccurate assessments of an individual's conduct.

As previously noted, LFR technology has significant issues with accuracy and bias, particularly with women and people of colour. While police forces' use of automated facial recognition is subject to the Freedom of Information Act, private facial recognition companies are not legally obliged to provide information about how their technology operates. We have requested information from Facewatch on any differential accuracy

260 Co-Op Using Facial Recognition To Spy On You, Big Brother Watch, YouTube, 26th July 2022, https://www.youtube.com/watch?v=i-B7NAX8zD4&ab_channel=BigBrotherWatch

261 Big Brother Watch Files Legal Complaint Against Co-Op's "Orwellian" Facial Recognition, Big Brother Watch, 26th July 2022, <https://bigbrotherwatch.org.uk/2022/07/big-brother-watch-files-legal-complaint-against-co-ops-orwellian-facial-recognition>

262 AEPD (Spain), PS/00120/2021, [https://gdprhub.eu/index.php?title=AEPD_\(Spain\)_-PS/00120/2021](https://gdprhub.eu/index.php?title=AEPD_(Spain)_-PS/00120/2021)

263 Dutch DPA issues formal warning to supermarket for use of facial recognition technology – Autoriteit Persoonsgegevens, 15 December 2020, <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-issues-formal-warning-supermarket-use-facial-recognition-technology>

264 Blog: Balancing People's Privacy Rights With The Need to Prevent Crime, Stephen Bonner, ICO, 31st March 2023, <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/03/balancing-people-s-privacy-rights-with-the-need-to-prevent-crime/>

rates or biases within the technology, but the company failed to respond. Neither does Facewatch address these issues anywhere else publicly. Without evidence of how the demonstrated risks of unfair bias in LFR technology are mitigated, it is reasonable to believe Facewatch's technology may be biased and could pose a disproportionate risk to women and people of colour.

Casinos and Gambling

Several casinos and bookmakers are using facial recognition under the guise of excluding addicted or problem gamblers from their premises.

Bookmakers

Entain Group, which has more than 3,000 betting shops across the country under the Ladbrokes and Coral brands, states in its privacy policy that it uses facial recognition in its physical premises as a way of identifying certain customers who enter.²⁶⁵ It claims that it may use facial recognition for several reasons, such as meeting its legal and regulatory obligations, conducting identity checks and preventing crime and loss. The regulatory obligations ostensibly include responsible gambling rules, in addition to anti-money laundering and anti-fraud laws. Meanwhile, the purpose of preventing crime and loss is outlined as covering fraud and theft, but also blocking “unfair practices” [which are not defined] and breaches of the company’s terms.²⁶⁶

It is not clear how many Entain Group shops make active use of facial recognition – but the industry body the Betting and Gaming Council has also promoted biometric scanning as a way to tackle problem gambling when bookmakers were caught out failing to meet their responsible gambling obligations.²⁶⁷

Casinos

As well as bookmakers, several casinos in the UK claim to make or have made use of facial recognition technology on their doors, including the Hippodrome on Leicester Square in central London and the high-end Clermont Club in Mayfair.^{268,269}

Although the Hippodrome told Big Brother Watch that it ceased using facial recognition in December 2020, following a pandemic-related temporary shutdown, it maintained a publicly available privacy policy on the technology that was updated in July 2021 for more than two years. It has since been deleted in May 2023 following correspondence with Big

265 Ladbrokes/Coral Privacy Policy, accessed 31st March 2023, <https://help.coral.co.uk/en/general-information/legal-matters/privacy-policy>

266 Ibid

267 Bookies’ Betting Sham As Sunday Mail Exposes Truth Of Gambling Self-Exclusion Initiative, Sunday Mail, 22nd December 2019, <https://www.dailyrecord.co.uk/news/scottish-news/gambling-self-exclusion-initiative-exposed-21143925>

268 Facial Recognition Policy, Hippodrome Casino, 15th July 2021, <https://web.archive.org/web/20230204100216/https://www.hippodromecasino.com/facial-recognition-policy/>, archived 4th February 2023

269 Privacy Policy, Clermont Club, accessed 31st March 2023, <https://www.clermontclub.com/privacy-policy>

Brother Watch. This policy, although now defunct, is an example of how the private sector use of facial recognition can pose a threat to individual's data rights and privacy.

It is not clear whether the threshold for a cheating exclusion is dishonesty that would breach the law, or whether activities such as card counting which are lawful but can get a player ejected from a casino would also be covered.²⁷⁰ The Hippodrome cited legitimate interests and legal obligation as its justification for using facial recognition – and pointed to Section 41, Paragraph 8 of the Gambling Act 2005 as allowing it to process biometric data to halt money laundering or the financing of terrorism.²⁷¹

However, Paragraph 8 of Section 41 of the Gambling Act appears not to exist, with the section halting at paragraph 5.²⁷² It is concerning that the Hippodrome casino's privacy policy about the use of facial recognition failed to accurately lay out the legal basis for its use of special category data in this way – and raises questions about the company's wider adherence to data rights given failed in this case to make sure its justification for processing biometric data is correct.

The Hippodrome only cited a legitimate interest justification under Article 6(1)(F) as its lawful basis for processing personal data with facial recognition, to exclude problem gamblers and to keep casinos safe and free of crime, and an additional Article 6(1)(C) justification claiming its legal obligations make the data processing necessary.²⁷³

Nowhere did the Hippodrome outline which of the Article 9 conditions it is also relying on to exempt it from the general prohibition of processing special category data under the UK GDPR.²⁷⁴ Organisations are required to both have a lawful basis under Article 6 and meet a relevant condition under Article 9 to lawfully process special category data, such as biometrics. The Hippodrome's complete failure to clarify the Article 9 condition it relies on underlines a worrying approach to data rights.

Necessity is also a key limb of Article 9 special category data processing, and the necessity of using facial recognition for self-exclusion is questionable. SENSE, the national self-exclusion scheme for problem gambling, does not collect special category data, such as biometric data, to run the scheme.²⁷⁵

270 Card Counting in Blackjack, PaddyPower, accessed 31st March 2023, <https://games.paddypower.com/info/card-counting-in-blackjack>

271 Facial Recognition Policy, Hippodrome Casino, 15th July 2021, <https://web.archive.org/web/20230204100216/https://www.hippodromecasino.com/facial-recognition-policy/>, archived 4th February 2023

272 Section 41, The Gambling Act 2005, <https://www.legislation.gov.uk/ukpga/2005/19/section/41>

273 Facial Recognition Policy, Hippodrome Casino, 15th July 2021, <https://web.archive.org/web/20230204100216/https://www.hippodromecasino.com/facial-recognition-policy/>, archived 4th February 2023

274 What Are The Rules on Special Category Data, Information Commissioners Office, accessed 3rd April 2023, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-rules-on-special-category-data/>

275 Privacy Policy, Self Enrolment National Self Exclusion [SENSE], July 2022, https://www.senseselfexclusion.com/assets/uploads/PRIVACY_POLICY_SENSE_Ltd-V01_July_2022.pdf

SENSE does warn in its privacy policy that particular venues and businesses may employ biometric identification methods, at their discretion – and asks enrollees to refer to relevant casinos’ policies. However the lack of specificity means that this would likely fall below the threshold of explicit consent to biometric processing.

It is also clear that facial recognition is not necessary to run a self-exclusion scheme, undermining the necessity limb of justifying special category data processing.

The concerning aspects of using facial recognition in gambling self-exclusion are exacerbated by the potential power imbalance relationship between somebody seeking help for problem gambling and a gambling company. Somebody who is distressed enough to seek a self-imposed ban from gambling premises should not be required to submit to biometric identification at certain venues, when the fact that most do not use the technology suggests it is not necessary. Further, operators should be mindful that even when operating LFR for people who opt into it, the majority of people whose data is processed will not have opted into or consented to biometric scans, meaning the privacy intrusion is neither necessary nor proportionate.

Facial Recognition Integrations to IP Camera Setups

Facial recognition is becoming an increasingly common capability offered on relatively cheap surveillance cameras on sale in the United Kingdom. CCTV cameras made by both Chinese state-owned companies such as Hikvision and Dahua, and Western surveillance brands such as Bosch, and AXIS offer facial recognition add-ons or integrations to either their cameras or the video management software they offer.

The prevalence of facial recognition as a feature of CCTV cameras available on the wider market risks normalising the technology regardless of the threat it poses to rights and privacy. If a technology is available it is more likely to be used. Facewatch, a plug-and-play system, markets itself on its simplicity and affordability, and likewise, the inclusion of facial recognition as a standard feature in connected cameras will only encourage the wider adoption of the intrusive technology because it is there.

In *Who's Watching You: The Dominance of Chinese State-Owned CCTV In The UK*, Big Brother Watch found that six per cent of secondary schools had facial recognition cameras made by Chinese manufacturers. Although all of the schools who said this in response to Freedom of Information requests clarified that they do not use facial recognition capabilities, the fact that a significant number have this Orwellian capability as part of their surveillance system shows how the technology is becoming increasingly normalised.

Hikvision and Dahua

Chinese state-owned surveillance camera makers Hikvision and Dahua already come with a host of ethical, rights and privacy threats regardless of their facial recognition offering. The companies are closely linked to atrocities in Xinjiang and have been described as providing the “infrastructure” for the surveillance of millions of Uyghur Muslims in the region. Local law enforcement has been offered ethnicity-based Uyghur-detecting technology by both brands, and Hikvision has made cameras geared towards monitoring torture victims in the “tiger chair”.

Both companies' equipment has also been found to have repeated cybersecurity flaws, with Italian investigators finding many Hikvision cameras pinging mysterious servers in China and several Western governments, including the UK, moving to remove the company's cameras from sensitive sites. Big Brother Watch has been campaigning for a complete UK Hikvision and Dahua ban since 2022, alongside calls for a wider CCTV review.

Hikvision is the dominant player in the UK surveillance market, while Dahua also has a

significant market share. Aside from the general ethical problems it poses, the companies' low prices for cameras which often include a host of AI-powered capabilities, such as "fight detection" and facial recognition, make algorithmic surveillance much more accessible to the general market.

A facial recognition camera from Hikvision or Dahua, via third-party vendors, can be bought for under £500 putting it in the reach of a huge number of individuals and businesses across the country. Suddenly, technology that was developed for and is heavily utilised by the Chinese state is easily accessible in the UK.²⁷⁶

Hikvision also has software partners which offer add-ons to its camera capabilities, including facial recognition tools. In late 2022, Big Brother Watch uncovered Hikvision's advertised partnerships with two companies that offered ethnicity recognition alongside facial recognition.

One of the companies is British facial recognition developer Faicetech, which was listed as a Hikvision partner on the Chinese company's website.²⁷⁷ After Big Brother Watch passed the information to the Guardian, Faicetech claimed that it had never worked with Hikvision and that the listing was made without its consent, while Hikvision claimed that it had nothing to do with technology partner listings which are made independently.²⁷⁸

Regardless of who was responsible for this particular product, or whether it has been pulled from use, this shocking example underlines how it is becoming increasingly easy and normalised to employ facial recognition software alongside internet connected cameras.

276 [Hikvision IDS-2CD7146G0-IZS DeepinView Series, accessed April 18th 2023, shg-uk.co.uk/Hikvision-DOME-IP-MPIXEL-INT-DN-IR-4MP-VF-DpInVw-iDS-2CD7146G0-IZS8-32mm](https://shg-uk.co.uk/Hikvision-DOME-IP-MPIXEL-INT-DN-IR-4MP-VF-DpInVw-iDS-2CD7146G0-IZS8-32mm)
[Stats annexe](#)

277 FaiceTech – Fast and Accurate Facial Identification, Hikvision, archived 5th July 2022, <https://web.archive.org/web/20220605150546/https://tpp.hikvision.com/Solution/SolutionDetail?Id=b522d82c-71d6-4bef-91bb-d86301704320&v=en>

278 Chinese Security Firm Advertises Ethnicity Recognition Technology While Facing UK Ban, The Guardian, 4th December 2022, <https://www.theguardian.com/world/2022/dec/04/chinese-security-firm-advertises-ethnicity-recognition-technology-while-facing-uk-ban>

Conclusions

The threat to everyone's privacy from facial recognition is not going away, and Big Brother Watch will continue to push back against the expanding surveillance state.

We stand against the expansion of Orwellian surveillance that is dangerously inaccurate and authoritarian. Our country should be free of surveillance without suspicion and unjustified attempts to infringe on our data and privacy rights.

Often these tools are targeted against minority communities, protestors and the vulnerable. Observations by Big Brother Watch at Metropolitan Police's LFR deployments found that black men make up the biggest proportion of those flagged by the LFR system and subjected to police intervention – this has included young boys and children who have been misidentified.

No legislation exists specifically to authorise, regulate or restrict the use of facial recognition surveillance. Instead, police forces and private companies rely on questionable interpretations of a patchwork of different acts and guidance in attempts to find legal justifications to make use of intrusive surveillance tools.

The absence of a legal mandate for the deployment of facial recognition surveillance, the disproportionate privacy impacts and the serious human rights issues it raises are why Big Brother Watch is calling for a ban on live and operator-initiated facial recognition. It is possible that there could be a strictly necessary and proportionate use case for the use of retrospective facial recognition, but that case has not yet been made. If it is made, primary legislation should be introduced to govern its use and implement robust safeguards that are standard for police use of other intrusive biometrics like DNA.

This report has outlined how police forces across the country are continuing to invest in and deploy various forms of facial recognition technology. The recent police-funded equitability study from the National Physical Laboratory appears to have only emboldened senior officers at the Met Police and South Wales Police to use facial recognition with increasing regularity on Britain's streets.

We are concerned about the growing normalisation of biometric identity checks in Britain, which is not limited to police use but is now expanding into a variety of inappropriate settings. We have documented how an increasing number of schoolchildren are being confronted by a face-scanning camera to pay for their lunch, while the Home Office seeks to use facial recognition with increasing regularity across immigration and visas.

In the private sector, we have seen the rise of companies seeking to be Google for faces, scraping the internet en-masse to biometrically analyse every photograph on the web, and

others who want to equip businesses across the country with custom facial recognition networks. The threat from facial recognition is not limited to state use of the technology but risks reaching into various areas of public life, with the potential for serious harms and rights impacts in people's private lives.

Orwellian, authoritarian surveillance tools must not be normalised as an aspect of daily life in Britain. On the contrary, public institutions should protect and uphold our data rights, and teach our young people in particular the importance of consent and control over their body data.

Despite the relentless drive by state and private state organisations to expand biometric surveillance over the past five years, there have been several victories in the fight against facial recognition since 2018.

From the Court of Appeal finding in the Bridges ruling that South Wales Police's use of live facial recognition in Cardiff was unlawful to the Metropolitan Police pausing deployments for two years in part due to pushback from Big Brother Watch, we have shown that this Orwellian technology will face strong resistance in the UK.

Since 2018, we have witnessed the atrocious uses of facial recognition surveillance around the world, whether in Russia to persecute democracy campaigners and abortion rights activists, or in China as part of a high-tech genocide against Uyghurs and ethnic minorities. Its relatively tentative use in the UK has been a total failure – proving persistently inaccurate, ineffective and discriminatory. Its adoption by police forces that are facing a crisis of public trust and deep-seated issues with racism, sexism and homophobia stands to only deepen the chronic issues in British policing.

But as in 2018, the key questions remain; do we want to live in a country where citizens are continuously watched, intrusively surveilled, and biometrically tracked?

Such a state would risk public freedoms, our democratic norms and our fundamental rights. The UK's use of facial recognition for surveillance makes us an outlier in the West.

New technologies put us at a crossroads for the future. If the UK is to positively embrace technology whilst protecting rights and democracy, parliamentarians must take action and legislate to prevent the serious harms we face and safeguard our rights.

Appendix – Police LFR Deployment Data Since 2019

MET POLICE DEPLOYMENTS SINCE 2019						
Event	Date	True Positives	False Positives	Wrong Interventions	Watchlist Size	People Seen
Piccadilly Circus	28/07/22	0*	0	0	6,858	16,440
Oxford Circus	16/07/22	0	1	1	6,747	36,420
Oxford Circus	14/07/22	2	1	2	6,713	34,360
Oxford Circus	07/07/22	3*	0	0	6,699	34,286
Leicester Square	10/03/22	0	0	0	6,793	10,740
Oxford Circus	28/01/22	7*	1	4*	9,756	12,120
Oxford Circus	27/02/20	1	7	5	7,292	8,600
Oxford Circus	20/02/20	0	0	0	7,268	N/A
Stratford Westfield	11/02/20	0	0	0	5,816	4,600
Romford Town Centre	14/02/19	2	7	2	1,998	?
Romford Town Centre	31/01/19	3	7	2	2,401	?
Islington	20/04/23	1	0	0	9816	3930
Camden	14/04/23	0	0	0	9744	6790
Camden	06/04/23	1	0	0	9764	5460
<p>^a Deployment was halted due to technical difficulties -----</p> <p>* Metropolitan Police deployment data logs alerts which they have not been able to verify (i.e. where they were unable to stop the individual and check their identity) as 'true alerts'. This is a mischaracterisation, as without verifying the individual's identity, officers have no way of knowing whether the match was true or false. We have not listed unverified alerts as true positives.</p>						

SOUTH WALES POLICE SINCE 2019 ²⁷⁹						
Event	Date	True Positives	False Positives	Wrong Interventions	Watchlist Size	People Seen
Speedway	13/08/22	0	0	0	245	20,929
Wales v Italy (Six Nations)	21/03/22	2	0	0	607	87,611
Slipknot (Motorpoint Arena)	22/01/20	n/a	n/a	n/a	97	?
Cardiff City v Swansea City (Cardiff)	12/01/20	n/a	n/a	n/a	39	?
Swansea City v Cardiff City (Swansea)	27/10/19	n/a	n/a	n/a	31	?
Elvis Festival (Porthcawl)	28/09/19	0	0	0	802	?
Elvis Festival (Porthcawl)	27/09/19	0	0	0	390	?
Neath Day of Action	27/09/19	1	0	0	453	?
Op SCEPTRE	11/09/19	1	0	0	418	?
Op SCEPTRE	05/09/19	1	0	0	414	?
Wales v Ireland (Six Nations)	31/08/19	3	13	0	792	?
County Lines	23/08/19	1	0	0	416	?
Wales v England (Six Nations)	17/08/19	7	7	0	803	17,688
Wales Airshow	07/07/19	2	5	0	702	11,265
Wales Airshow	06/07/19	3	4	0	702	21,325
Take That	08/06/19	2	5	0	791	18,358
Operation Sceptre	07/06/19	0	0	0	2	?
Spice Girls Concert	27/05/19	6	9	1	781	18,931
Operation Cristo	16/05/19	0	0	0	424	?
Day of Action (location unknown)	09/05/19	0	0	0	480	2,164
Catfish and the Bottlemen concert (Motorpoint Arena)	05/05/19	0	0	0	414	3,041
Day of Action (location unknown)	09/04/19	0	0	0	451	?
Day of Action (location unknown)	05/04/19	3	1	1	413	2,243
Wales v Ireland (Six Nations)	16/03/19	0	7	1	738	14,142

²⁷⁹ All Deployments since 2017, South Wales Police, accessed 4th April 2023, <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/live-facial-recognition/all-previous-deployments-since-2017.pdf>

Wales v England (Six Nations)	23/02/19	4	8	1	700	18,359
Operation Cristo' (Location unknown)	10/01/19	2	0	0	401	?

