A thematic report published by
Policinginsight

June 2024



Facing the future

The rise of facial recognition in policing

Information and acknowledgements

Credits



AUTHOR
James Sweetland
Contributing Writer for Policing Insight



EDITING
Keith Potter
Editor of Policing Insight



PRODUCTION
Ian Barrett
Director of Publishing and Product Development, Policing Insight



DESIGN
David Devonport
Freelance Designer

'Facing the future: The rise of facial recognition' – a thematic report, researched and produced by Policing Insight

Welcome to our latest report, which aims to go behind the headlines and beyond the simplified facial recognition (FR) debate that we see in so much of the media today. This report highlights the types of FR in use by policing and others around the world, and explores the big debates around that use. Many thanks to the 34 stakeholders – including policing practitioners, academics, regulators and suppliers – who agreed to be interviewed by report author James Sweetland and shared their views and expertise on this complex issue. We are also grateful to NPCC Chair Chief Constable Gavin Stephens for his insightful foreword to the report. We hope you find the report an interesting and valuable exploration of FR.
Ian Barrett, Director of Publishing, Policing Insight

Policinginsight

Policing Insight is the leading platform to keep up with the latest in progressive policing. It is where the global police and criminal justice community both consume and share knowledge, opinion and analysis. Policing Insight's subscription community consists of government, policing, third sector, academia and industry, all interested in working towards better policing outcomes.

If your organisation would like to commission an independently researched and written report from Policing Insight on an important policing and criminal justice topic, please contact **enquiries@policinginsight.com**

Read more Policing Insight reports at **policinginsight.com/reports**

Special thanks

We are hugely grateful to the 34 expert stakeholders who gave up their time to be interviewed, without which we would not have been able to produce this report:
Dr Andrew Chen, Senior Research Fellow, Koi Tū: The Centre for Informed Futures, University of Auckland; **Lindsey Chiswick**, Director of Intelligence, Metropolitan Police and National Police Chiefs' Council (NPCC) Lead on Facial Recognition; **Tony Eastaugh**, Biometrics and Surveillance Camera Commissioner; **Marie Eneman**, Associate Professor in Informatics, Department of Applied IT, University of Gothenburg; **Dr Elizabeth Farries**, Co-Director, UCD Centre for Digital Policy; **Nick Fisher**, CEO, Facewatch; **Professor Clare Garvie**, Senior Associate, Center on Privacy & Technology, Georgetown University Law Center; **Andy George**, President, National Black Police Association; **Dr Asress Gikay**, Senior Lecturer in AI, Disruptive Innovation and Law, Brunel Law School; **Inspector Crystal Govers**, Metropolitan Police; **Baroness Hamwee**, Chair of Lords Justice and Home Affairs Committee; **Ella Jakubowska**, Head of Policy, European Digital Rights Network; **Emily Keaney**, Deputy Commissioner, Regulatory Policy, Information Commissioner's Office; **Patricia Kosseim**, Information and Privacy Commissioner of Ontario; **Professor Kyriakos Kotsoglou**, Associate Professor, Northumbria Law School; **Chief Philip Lukens**, AI and Policing Expert, International Association of Chiefs of Police; **Dr Nessa Lynch,** Matheson Lecturer in Law, Innovation & Technology, University College Cork; **Dr Neil McBride**, Reader in IT Management, DeMontfort University; **Abdul-Hye Miah**, Senior Lecturer in Criminal Justice Studies, University of Northampton; **Alun Michael**, former Police and Crime Commissioner for South Wales; **Stuart Moss**, Sales Director for Public Safety, NEC Software Solutions; **David Murphy**, Assistant Commissioner, Irish Data Protection Commission; **Andrew O'Sullivan**, Chief Information Officer, An Garda Síochána; **Professor Marion Oswald**, Professor in Law, Northumbria Law School; **Lauren Perry**, Policy Specialist at the Human Technology Institute, University of Technology Sydney; **Ira Reese**, Chief Technology Officer, Global Security and Innovative Strategies; **John Riemen**, Lead Biometric Specialist, Dutch National Police; **Inspector Karl Roberts**, South Wales Police and Project Manager, National Biometrics Function; **Professor Fraser Sampson**, Professor in Governance and National Security, Sheffield Hallam University and Non-Executive Director at Facewatch; **Madeleine Stone**, Senior Advocacy Officer, Big Brother Watch; **Dave Sumner**, Director for Privacy, Facewatch; **Professor Paul Taylor**, National Police Chief Scientific Adviser, NPCC; **Phil Thomson**, CEO, Auror; **Chief Superintendent Sean Wilson**, Metropolitan Police.

Copyright © 2024 CoPaCC Ltd / Policing Insight

Images from Metropolitan Police LFR deployment copyright Policing Insight/CoPaCC Ltd and with thanks to photographer Kevin Poolman. Other images: unsplash, pixabay, pexels

Facial recognition Stakeholder voices

"From a strategic perspective, the question we've got to keep asking ourselves is: 'Are our processes and frameworks keeping track with the speed of technological advances?' The stuff we've put in place today – the mitigations, the frameworks, the accountability, the scrutiny – is that fit for tomorrow, bearing in mind the advances that are already taking place?"

Tony Eastaugh
Biometrics and Surveillance Camera Commissioner





"There's still a problem if the system returns possible matches and the human analyst knows those are in rank order (from most to least likely matches). There's going to be incredible cognitive bias towards agreeing with the findings, as opposed to performing any sort of independent systematic review."

Prof Clare Garvie
Senior Associate,
Georgetown University Law Center

"If we look at what the police are actually doing, they're addressing a lot of concerns. But the technology itself is moving so fast. That means the police need to up their game and be proactively open and transparent, while using this technology."

Abdul Hye-Miah
Senior Lecturer in Criminal Justice Studies, University of Northampton





"My [family member] hasn't got the skills and ability to make themself known to policing. But if they walked past an LFR camera and were a missing person, it would identify them and allow the engagement team to give support. And certainly in South Wales, we use LFR's capability to locate and trace vulnerable and at-risk people… LFR is not just about identifying the bad guys and girls."

Insp Karl Roberts
Project Manager, South Wales Police

"With LFR there's a fleeting engagement of a face which is immediately deleted by the technology if you're not wanted. And you go on your way, you wouldn't know [it's scanned you]. It takes literally milliseconds."

Lindsey Chiswick
Director of Intelligence Met Police,
and NPCC Lead on Facial Recognition



"It's a mass surveillance tool that turns the streets of Britain into police line-ups and our faces into barcodes… The fact that every single person has their sensitive biometric data scanned and processed as an ID check is completely disproportionate. We see no way that it could ever be used in a proportionate way."

Madeleine Stone
Senior Advocacy Officer,
Big Brother Watch

"Even though a trained facial examiner can go through thousands of images a day, it becomes very impractical very quickly to go through that kind of volume… Even in relatively small investigations, we could have thousands or tens of thousands of hours of footage."

Andrew O'Sullivan
Chief Information Officer, An Garda Síochána



Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition Stakeholder voices



"However much the forces say that they're making it clear to the public that they're deploying the technology, I have no confidence that's obvious to people. The Met, in particular, when they were talking to us, relied on the fact that there is stuff on social media."

Baroness Hamwee
Chair of the Lords Justice and Home Affairs Committee

"I think in five years we'll have a national cadre of vans housed in strategic locations across the country and brought out to keep people safe at major events. They'll be used as an intelligence tool to support areas where they're needed."

Professor Paul Taylor
National Police Chief Scientific Adviser



"What's missing in FR is what's not missing around DNA and fingerprints. At this point in time, FR in the United States is more or less equivalent to the Wild West."

Ira Reese
CTO, Global Security Innovative Strategies



"FR today is kind of like when the dot-com craze hit in the 90s. Everybody was all over it for five years and then over time, it began to take shape. But it was the Wild West for a good five years."

Chief Philip Lukens
AI and policing expert, International Association of Chiefs of Police



"My personal opinion, when it comes to bias, is that if it's not already solved, it will be solved in the next three to five years. I think the bias issue is probably overstated and it's an unreliable argument for the civil liberties groups, because it will go away at some point."

Dr Andrew Chen
Senior Research Fellow, University of Auckland





"I think we're setting up LFR to disproportionately impact the Black community in London at the minute. At any other time that would be bad enough. But with the crisis in confidence and the [current] feeling in the community, I think now's definitely the wrong time to deploy stuff into almost singular Black communities rather than other places."

Andy George
President, National Black Police Association

"The police have amended their policies to try and deal with the issues the court [found]… But there's no definitive conclusion on whether everything's fine now. It would need another court case to decide if what's been done has satisfied the issues Bridges identified."

Professor Marion Oswald
Professor in Law, Northumbria Law School



Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Executive summary

In this major Policing Insight thematic report, we explore how facial recognition (FR) is being used in policing and for public safety purposes. We explain exactly what FR is, how police forces across the Western world are deploying it, and the complex debates around its use.

These findings reflect a wealth of research and evidence gathered over the past few months. This includes dozens of news reports, studies and police policy documents, interviews with 34 leading experts on FR, and behind-the-scenes access to an FR deployment hosted by the Metropolitan Police in London.

So what is facial recognition?

Many people will have heard the term 'facial recognition', but outside of technical specialists and subject matter experts, how much do we really understand about the different applications of the technology, the standards that are used to ensure accuracy, and how widely FR is in use by police and other organisations?

In the first section of this report, we explore some of these key points. We look at the three main types of **facial recognition used by police** – live FR (sometimes described as FR surveillance), retrospective FR (comparing suspect images to a database after an event), and operator-initiated FR (an app set to be rolled out across England and Wales).

We examine the ever-increasing **private sector use of FR**, especially by companies in the retail sector, such as Facewatch and Auror. However, FR isn't limited to the shopping aisles; stadia, casinos and factories also deploy this technology, including its use more than 20 years ago at the 2001 Super Bowl.

And while the issue of current FR use is uppermost in many minds, there are a range of possible **future applications** too, such as body-worn video cameras, drones, or FR CCTV networks, and the potential for other tech that can identify emotion or use multiple biometrics at once.

What's happening where?

The second section of this report looks at how FR is currently used around the world, and the different approaches by individual countries and jurisdictions, starting with **England and Wales** – viewed either as a leader or an outlier, but agreed by all as one of most advanced Western states in its adoption of the new technology.

Australia and the US have both previously experimented with LFR, but our research suggests there is a lack of clear understanding about the current police use of the technology, with the US in particular described as taking a "Wild West" approach. By contrast, in **the Netherlands** the country's well-established police RFR programme involves a significant amount of human oversight and intervention, with no LFR used yet.



There are signs of increased use of RFR in both **New Zealand and Canada**, but little evidence of live versions being deployed any time soon. In **Ireland and Sweden**, political leaders are pushing for expanded use of FR (though only Sweden has announced plans to use LFR); the **EU AI Act** may have significant and unexpected implications for the use of LFR in these and many other European countries too.

Understanding the big debates

In the third section of this report, we identify and consider some of the major discussions and debates around the adoption and deployment of FR. Key to all of these is the real **operational value** of the technology. Alongside enforcement (to help identify and arrest wanted people), deterrence, public reassurance, and ensuring people comply with legal conditions, there are also interesting non-crime benefits, such as making it easier to find missing people, and the improvements in speed and effectiveness offered by RFR and OIFR.

However, these benefits also come with significant risks and concerns, most notably **bias and accuracy**. While this report highlights evidence that FR systems and algorithms are becoming more accurate over time, there remain worrying cases internationally that appear to show how FR's deployment can lead to unequal outcomes.

There is also the issue of the **human-in-the-loop approach** – human oversight seen as essential to a trustworthy FR system – and whether such measures will actually add or remove harmful biases.

Intrusion and privacy remain substantial concerns around the use of FR, especially in public spaces. Police in England and Wales point to the auto-deletion of innocent people's data and attempts to publicise LFR deployments as ways to mitigate this, but others remain sceptical. That scepticism is also fuelled by **legal and regulatory uncertainty**, with legislators failing to keep pace with the rapid developments in FR use, and policing's attempts to fill the gaps with guidance or policies work still leaving important questions about oversight and the often complex legal basis for FR use.

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Foreword

FR is one of the biggest breakthroughs since DNA



Chief Constable Gavin Stephens, National Police Chiefs' Council (NPCC) Chair, outlines the crime fighting potential of facial recognition, and policing's pledge to balance investigative opportunities with privacy and transparency.

How we embrace scientific developments will be the single biggest driver of reform in policing in the coming years. Technology is all around us, moving at an awe-inspiring pace, and the reality is that we need to keep up with it, or risk falling behind.

Embedding various technologies into policing will ensure we offer the best possible service to our communities, by putting their safety first, detecting crime more efficiently and locating dangerous offenders more effectively.

We are proud to police by consent in this country and our journey towards greater productivity and a more technologically driven service must be one the public takes with us. The communities we serve must be informed and engaged in discussions around new tools, devices and platforms or we're failing at first hurdle.

Earlier this year, I was proud to sign the first ever **Police Industry Charter** which commits us to working with industry specialists, academics, government and experts to deliver digital improvements and advancements. The Charter means I can say with absolute certainty we're using all the expertise available, understanding all of the ethical, concerns, constraints and limitations.

The exploration of facial recognition (FR) technologies has been no different and we will continue to work with our communities and critics alike as we progress.

A real eye-opener

Some of you reading this will know more about FR than others, and for some readers this piece may be a real eye-opener into how policing is transforming and becoming more intelligence driven and precise.

As you read about the various types of FR, I'd ask you to do so with an open mind. Think carefully about where your data and biometrics may already be, who might be using them and why, and compare this to the police approach, which is tightly legislated, constantly reviewed, and in the case of live facial recognition (LFR), deleted after 24 hours.

There are many prominent voices in the FR world but I'd ask you pay special attention to Lindsey Chiswick, Director of Intelligence for the Metropolitan Police Service and the NPCC Lead for FR.

Her leadership and oversight of LFR is second to none, and her force is one of two currently trialling the technology, with huge successes to date. Recent data tells us that since LFR was rolled out in London, it's been responsible for one arrest every two hours.

And there are other types of facial searching which you will read all about. All forces have the capability to carry out retrospective searches which sees a CCTV or image cross-referenced with the custody image database to find a potential match. A recent study by South Wales Police found that on average, an officer will take 14 days to identify a suspect without this technology, but when using it can find a match in as little as several hours.

> **"FR [is] one of the biggest breakthroughs for crime detection since the discovery of DNA. The highly precise nature of the way it works and its constant delivery is a game-changer."**

Results like this make FR one of the biggest breakthroughs for crime detection since the discovery of DNA. The highly precise nature of the way it works and its constant delivery is a game-changer.

These results are exactly what our communities want to see and what victims deserve. Dangerous and violent offenders who are trying to evade justice are being located, identified and arrested.

Sadly, the conversation about FR is tainted by surveillance states where there are widespread reports of human rights abuses. The way UK policing is using this technology couldn't be more different and I hope the conversation begins to shift, placing the work we are doing and the positive results we are seeing at the centre.

I'm confident we are and will remain a world-leader in this area and that engagement with both sides of the discussion will continue. There is of course a need to balance investigative opportunities with the right to privacy.

Our communities are right to ask questions and raise any concerns with us and here are my guarantees to the public on behalf of policing.

We will always be open and transparent in the way we use this technology. LFR for example is always intelligence driven, and trained officers will always make the final decision, no matter what.

We'll never store or hold biometric data without a legitimate and legal reason to do so, and anyone walking by whose image is captured on camera can be assured their biometrics are deleted within 24 hours.

Unlike surveillance states, we will always welcome scrutiny and there are many processes in place to govern and challenge FR, which we will always engage with.

We'll continue to work closely with the National Police Chief Scientific Adviser, Professor Paul Taylor (also featured in this report), as well as with ethics panels, individual chief constables, police and crime commissioners, and deputy mayors. We'll also share the work and findings of our Science and Innovation Coordination Committee, who oversee and scrutinise all of our work in the world of science and technology.

The public tell us they want to see us fight crime and be visible in the communities we serve. To deliver a first-class modern policing service that's fit for purpose, technology needs to be at the forefront, and we need to familiarise ourselves with FR.

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Contents

Easy content navigation!
- **Click article titles** to jump to the required article page.
- **Click 'Back to contents'** links at the bottom of each page to return to Contents page







8 **Introduction**

9 **1: What is facial recognition?**
There are many types of technology that can identify individuals based on biometric attributes such as fingerprints, face, and voice; understanding their uses and limitations is vital to effective policing.

11 **What is FR – and how do the police use it?**
13 **The basics you need to know**
15 **Facial recognition on deployment**
19 **Outside the police: how the private sector is using FR**
22 **The future of facial recognition**

25 **2: Facial recognition around the world**
The international picture in relation to the use of FR is both varied and complex, and the opportunities and challenges are prompting lengthy debates and driving different approaches to the technology.

27 **England and Wales: world leader or global outlier?**
32 **Australia and the US: early experiments in LFR**
35 **The Dutch model: a unified national approach**
37 **New Zealand and Canada: little chance of 'live'**
40 **Ireland, Sweden and the EU AI Act**
43 **Approaches to FR around the world**

47 **3: The big debates**
FR is a rapidly evolving technology; so how great are the potential benefits, what are the risks, and where is the current conversation on bias, regulation, privacy and the role of humans in an AI world?

49 **The operational value of facial recognition**
53 **Biased systems or accurate tools?**
57 **The human in the loop**
60 **Intrusion and the threat to privacy**
63 **Legal and regulatory uncertainty**

66 **Conclusion**

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

A hot topic for policing today

In this report, Policing Insight explores exactly what facial recognition really is, how FR is deployed by law enforcement across the Western world, and the big debates around use of the technology.

The debate around facial recognition (FR) is constantly in the news, especially when it comes to its use by law enforcement or for public safety. This technology is increasingly common across the world, whether in Western states or authoritarian nations (in this paper, we generally focus on the former). At the same time, there's been a growing push for regulation and oversight, with the recently passed EU AI Act being the foremost example of this.

It's no surprise therefore that FR is a hot-topic issue for policing today and for the foreseeable future. It's for this reason that FR is the focus of our newest thematic report.

In this detailed paper, we aim to do three main things for you, our readers. First, **we explore exactly what FR really is**. That includes the key fundamentals of the technology: how it works, live vs retrospective FR, the key statistics, and what the future of biometrics could look like. We also go inside one of the Metropolitan Police's FR deployments, with exclusive behind-the-scenes access to show you how it is really used on the ground.

Next, **we take a global view**, examining how FR is deployed by law enforcement across the Western world. Through detailed case studies in a wide range of countries – England and Wales, Australia, New Zealand, Canada, the US, the Netherlands, Sweden, and Ireland – we explore the different approaches to FR and how advanced its use is in each jurisdiction.

And finally, **we focus on the big debates around FR**. You may have seen some of Policing Insight's FR coverage before, or other comments elsewhere in the media. But in this report, we dive deeper into the really complicated questions this debate throws up. What are the actual operational benefits of FR? What are the privacy and bias implications of this tech? How do we keep humans in the loop, and do we need better regulation or legislation?

> **"Our ability to do all of this and take on all of these questions is ultimately down to the generosity of the 34 people we interviewed for this report."**

Our ability to take on all of these questions is ultimately down to the generosity of the 34 people we interviewed for this report. We thank them for their contributions and the time they gave to speak to Policing Insight. Their insights are at the heart of what we believe will make this paper so valuable.

Our approach has been a deliberately broad and inclusive one. We spoke to police operational leaders deploying this evolving tech, politicians and regulators scrutinising its use, legal and academic experts, highly critical activist groups, and many more besides. All of their insights are embedded within this paper to give all sides of the story, ranging from those trying to sell FR to those who're working hard to try and stop it.

Overall, our hope is that – for readers across policing and beyond – this report is a resource you can keep coming back to. From insights into how the Met and South Wales Police have grown their use of FR, to the intricacies of bias, the ongoing discussions around privacy, and the potential operational benefits and challenges of FR, we cover the key issues in a level of detail that will keep you informed and up to date.

As everyone we interviewed agreed – from those most supportive of FR, to its strongest critics and sceptics – this technology isn't going away, it's growing. This report can be your guide, offering the key to understanding this essential and often contentious debate.



Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

1

What is facial recognition?

What is facial recognition? Stakeholder voices

"The police don't have the resources to deal with low-level [retail] crime, but often that comes with violence and aggression too. So, let's come up with a solution that deters and prevents the horrible guys from going into stores. That's what we did. The model was to commoditise FR so it's affordable for retailers who want to take it."

Nick Fisher
CEO, Facewatch



"It's very difficult to cheat live facial recognition. For me, it's a significant step forward in how we do proactive policing across the command. We will always do it with ethics and make sure our policing model is proportionate. And we will do it within the confines and boundaries of the legislation that's available to us."

Ch Supt Sean Wilson
Borough Commander, Metropolitan Police





"There may be particular considerations in those use-cases which enable you to bake in data-protection-by-default approaches. But generally, we're still talking about the same principles around data protection in those cases. It's all the same rule book."

Emily Keaney
Deputy Commissioner for Regulatory Policy, UK Information Commissioner's Office

"After an event has occurred, that security guard or store manager would report what occurred into the Auror platform. We help them with that entire reporting process and gather the evidence (which could be witness statements, receipts, video footage) and capture all that in one place. They could then provide it to the police with a click of a button."

Phil Thomson
CEO, Auror



"The deployment in Croydon was to tackle serious and violent crime. This year, Croydon has the highest murder rate. It has the highest number of knife crime-related offences. It has a blossoming night-time economy, and with that comes problems such as violence against women and girls. That was the intelligence case that sits behind why we wanted to deploy there."

Lindsey Chiswick
Director of Intelligence, Met Police, and NPCC Lead on Facial Recognition





"The default position is that we're the second most surveilled society in the world… But, as time goes on and people start to understand more about how FR could be used against them in different formats, I think we're going to get some very difficult questions back from the public."

Tony Eastaugh
Biometrics and Surveillance Camera Commissioner

"The thing you need to understand is that the technology varies… There are so many factors that mean it's not a homogenous technology. You have to look at the individual suppliers."

Dr Neil McBride
Reader in IT Management, DeMontford University



"We are the UK's second largest police force for the volume of incidents of retail crime that we record… I've looked at academic data on offending patterns, what different offender cohorts do, whether they're opportunist, prolific, etc. I've based the sharing radius on that information to ensure it's not a sledgehammer to crack a nut. It's proportionate to the offence."

Dave Sumner
Director for Privacy, Facewatch

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

What is FR and how do the police use it?

There are many types of technology that can identify individuals based on their biometric physical and behavioural attributes, such as fingerprints, face, and voice. Understanding the uses and limitations of each is vital to effective policing.

To understand facial recognition (FR), you first have to take a step back and think about biometrics more generally.

These technologies, **according to the UK Parliamentary Office for Science and Technology**, "identify individuals based on their distinguishing physical and behavioural attributes, such as fingerprints, face, and voice". This can also include attributes such as a person's walking gait, and even the way they use a keyboard.

There are different ways to categorise biometrics within that. **A recent Alan Turing Institute study** offers three examples of this:

- **Soft vs hard:** hard biometrics, such as fingerprints, can identify specific people much more easily than soft ones (eg walking gait or eye colour).
- **Physiological vs behavioural:** physiological biometrics rely on physical features (eg face or DNA), whereas behavioural biometrics are closer to 'patterns' – for example, an individual's voice or walking gait.
- **Direct vs remote systems:** direct biometric systems such as fingerprint sensors need physical touch or contact, while remote ones – including FR – don't.

The face

When the face is used as your biometric, it usually falls into the hard, physiological and remote categories above. That's not always true though. For example, if a facial scanner is trying to read emotions from a face, it is still remote – but it also fits in the soft and behavioural categories.

This means the face can be used in different ways within biometric systems. The same Alan Turing Institute study talks about four types of systems:

- **Verification:** this is about so-called '1:1 matching', with a system that uses an image of someone's face to check they're who they say they are. For example, to unlock a smartphone, the device might scan an individual's face and compare it to the record for 'iPhone owner'. Effectively, it's comparing the image to a database of just one person.
- **Identification:** this is '1:N' or 'one-to-many matching'. It compares the face of an unknown person, perhaps someone walking by a camera, to a larger database of faces, and identifies whether the person is a match for anyone on an existing list. This is usually what we're referring to when we discuss the police use of FR.
- **Classification:** this is about using biometrics to categorise people – for example, looking at someone's face and trying to determine their ethnic group, gender or similar. In the context of faces, both classification and inferential biometrics (see below) are also sometimes referred to as '**facial characterisation**'.
- **Inferential:** this looks at someone's biometric data, such as their face, and tries to read their emotions from that. It's a highly controversial area, and generally not used by law enforcement at this stage.

If this all sounds incredibly complicated, that's probably because biometrics is a complex field, one in which many experts disagree on exactly how to categorise things. But for our purposes, things are a little simpler.

In this report, we're focused (almost always) on systems that use the face for identification purposes to tackle crime or promote public safety, whether it's deployed by law enforcement and policing, or private actors.

More than just an algorithm

It's important not to focus solely on artificial intelligence (AI) and algorithms. Yes, effective FR systems rely on high-quality algorithms. They need to be good at identifying similar faces while also avoiding accidentally reporting that two different people are the same individual.

> **"An FR system will work better with a high-quality database; if a 'watchlist' has excellent photos of suspects' faces, the system is more likely to get good matches. Equally, good images need to be fed in for identification."**

But other things matter too. For example, an FR system will work better with a high-quality database; if a 'watchlist' has excellent photos of suspects' faces, the system is more likely to get good matches. Equally, good images need to be fed in for identification. If the FR camera takes a grainy, low-resolution image of someone in the middle of a blizzard, it will be more difficult to get a match than from a high-quality image on a sunny day.

It's also about how a system is used. How high a threshold should be set for a 'hit' to be reported? Should the system present one or many potential matches? How well trained are the human operators? Do they have the confidence to overrule the tech when it makes mistakes or do they blindly follow the computer? All of these factors count.

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

What is facial recognition?

Three types of police FR

For policing's use of FR, we'll refer to three main types of technology, using the terms that police in England and Wales (as well as many others around the world) tend to stick with.

The first is **retrospective facial recognition (RFR)**. According to the **UK Home Office**: "RFR is used after an event or incident as part of a criminal investigation. Images are typically supplied from CCTV, mobile phone footage, dashcam or doorbell footage or social media. These images are then compared against images of people taken on arrest to identify a suspect."

RFR is by far the most common use of FR covered in this report. In essence, it's about taking images from crime scenes or other incidents and comparing them to existing databases. For example, a CCTV image of a wanted suspect is compared to a police database, with the RFR deciding if any faces match. The key point is that it's not 'live', nor is it surveillance.

> "RFR is used after an event or incident as part of a criminal investigation. Images are typically supplied from CCTV, mobile phone footage, dashcam or doorbell footage or social media. These images are then compared against images of people taken on arrest to identify a suspect."
>
> **UK Home Office**

The second is **live facial recognition (LFR)**. To return to another Home Office explanation: "The technology uses live video footage of crowds passing [by] a camera and compares their images to a specific list of people wanted by the police." LFR remains much more controversial than RFR; it's far less widely used in the Western world.

LFR is distinct from RFR in two senses. First, it is 'live' (some say 'real-time') rather than post-event. This means that someone flagged up as a match will face immediate consequences – whether being stopped, arrested or denied entry somewhere. That increases the potential for mistakes.

Secondly, it involves some type of surveillance over (usually) public spaces. As a result, many people who are not on the relevant list will be captured on camera and have their faces scanned. An RFR system, by contrast, generally compares one image (or several images of a single individual) to a database – meaning 'innocent' people are rarely affected. And LFR offers much more potential for 'chilling effects', if people in public spaces fear being surveilled.

The third and final type is **operator-initiated facial recognition (OIFR)**. The Home Office describes it as: "A mobile app that allows officers, after engaging with a person of interest, to photograph them and check their identity where they are not sure, without having to arrest them and take them into custody."

OIFR has been trialled in a number of forces, but is now **set to be made available** to all forces in England and Wales sometime this year.

It's an interesting example of where the temporal part of the LFR vs RFR debate can become complicated. If an officer takes a photo and runs it through a database, it's clearly not surveillance in the same vein as LFR; but it's not strictly 'retrospective' either, as it's used during a stop, rather than post-event.

Equally, while Policing Insight understands that OIFR is used for facial identification now – comparing a face to the whole database (one-to-many or 1:N matching) – it could plausibly be used for verification instead: comparing the person to a specific suspect's record, to check if it is a match.

And two more...

There are, technically, two other types of FR, as referred to in a **Met Police guidance document**. These are the covert uses of LFR – Covert Real-Time Facial Recognition Surveillance (CRFRS) – and of OIFR – Covert Operator-Initiated Facial Recognition Surveillance (COIFRS.)

A number of police forces in England and Wales have refused to comment on any potential use of covert FR, when **sent Freedom of Information requests**. Given the lack of available public information on both types, we have not explored covert FR in this report.

CLICK HERE
Report
Biometric Technologies
An overview of these technologies, their applications, and the policy challenges that arise from their use
researchbriefings.files.parliament.uk

CLICK HERE
Report
The Future of Biometric Technology for Policing and Law Enforcement
Exploring the future of biometric technology for UK policing
cetas.turing.ac.uk

CLICK HERE
Report
How Does Facial Recognition Work?
A primer on facial recognition technology
csis-website-prod.s3.amazonaws.com

CLICK HERE
Report
Police use of Facial Recognition: Factsheet
Home Office factsheet on police use of facial recognition technology
homeofficemedia.blog.gov.uk

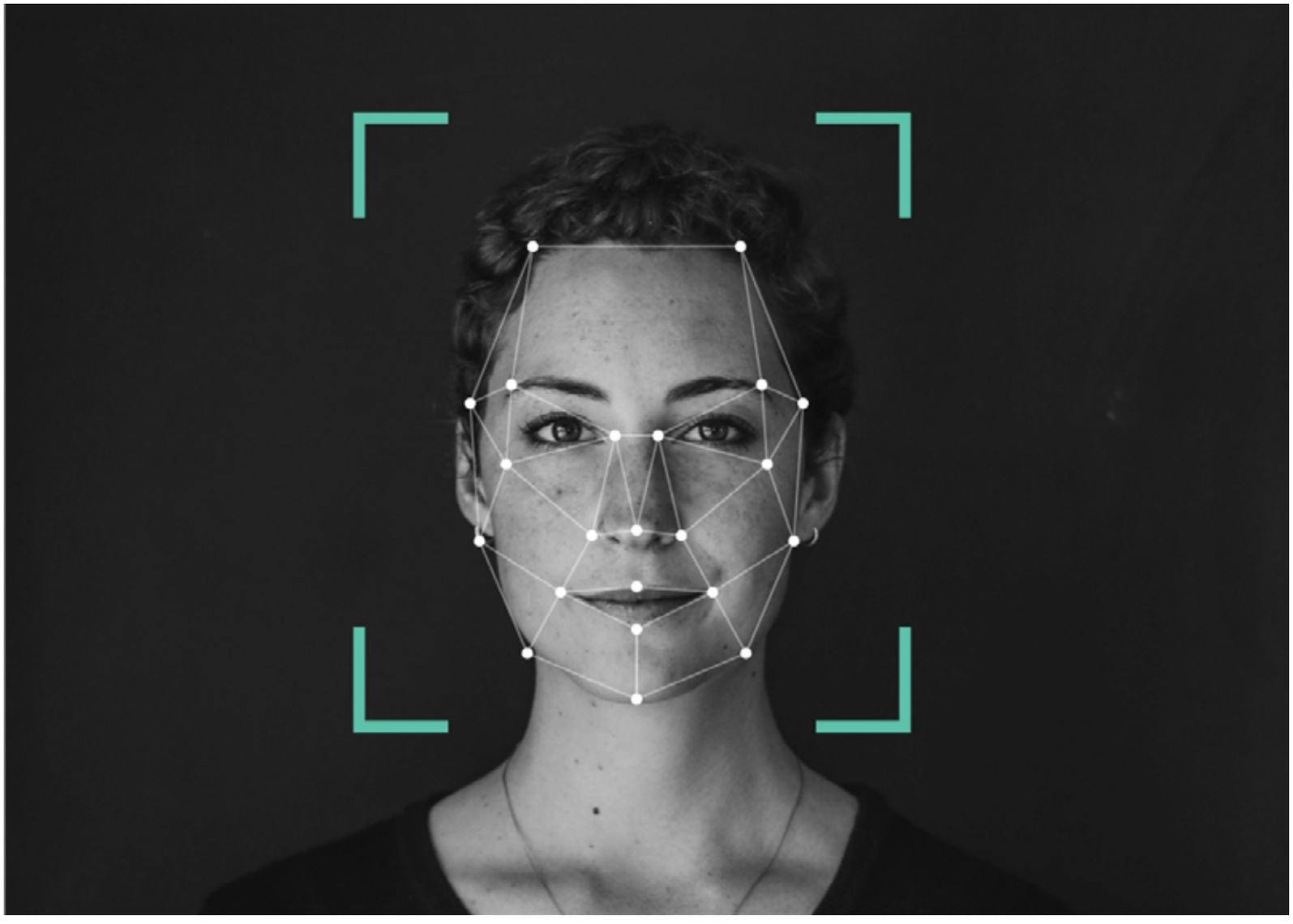
CLICK HERE
Report
Facial Recognition Cameras in London & Locations
A Freedom of information request
met.police.uk

CLICK HERE
Policy
MPS policy – retrospective facial recognition system
Establishes policy and standard operating procedures for the use of the MPS Retrospective Facial Recognition System.
met.police.uk

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

The basics you need to know

This beginner's guide to facial recognition explains all the essential terms and phrases you need to understand – from true positives and false negatives, to threshold settings and landmark studies.



The public conversation about facial recognition (FR) can sometimes be caught between two extremes. There's plenty of complex discussion about FR algorithms that is enormously technical or even impenetrable to those without a background in statistics. However, the debate can also go too far the other way, with reports missing out some of the key terms that are really important to properly understanding FR.

In this short piece, we'll explain the essential terms and phrases; from true positives and false negatives, to threshold settings and landmark studies, this is a beginner's guide to this complex topic.

Positives and negatives

At the most basic level, there are numbers that don't require much explanation at all. For example, when a live facial recognition (LFR) system is operating, it will compare an image of someone to a database of faces. At a recent **Met Police deployment** in Ealing, there were 13,204 'wanted' faces on the watchlist and the cameras scanned an estimated 2,446 faces of people walking by.

However, measuring accuracy becomes more complicated. The vast majority of those scanned will be 'true negatives', people not wanted by police (and therefore not on the police watchlist) who are scanned and correctly identified by the system as a 'non-match'. But the three terms that are of greater importance here are true positives, false positives, and false negatives.

A true positive is what operators are looking for when using an FR system. It means that the image taken – whether via a live camera shot or a photo – has been matched to someone in the

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

What is facial recognition?

database, generating a 'positive result or alert'. And, crucially, it means the system has got it right. It's 'true' – the two images are indeed the same person.

A false positive means the system has got it wrong. The FR system identifies a match ('a positive'), but it's not actually the same person – hence 'false'. This can be highly damaging, as it can lead police to target an individual who has nothing to do with the crime.

A false negative is another example of the system getting it wrong. The FR system says there is no match ('a negative'), but the two images are actually the same person – hence 'false negative'. For policing, that can potentially harm an investigation, as it ignores a person already on a policing database – meaning useful intelligence may be overlooked.

> **"The thing you need to understand is that the technology varies… There are so many factors that mean it's not a homogenous technology. You have to look at the individual suppliers."**
>
> **Dr Neil McBride, DeMontfort University**

When using FR, accuracy is all about trying for the highest possible true positive rate and the lowest possible false negative and false positive rates.

How accurate are these systems?

Ultimately, different FR algorithms vary in terms of their performance. Even when used in exactly the same conditions, a more effective algorithm could have a much higher true positive rate than a less effective one.

There is enormous variation in the market, with different companies offering algorithms that are more or less effective. As Dr Neil McBride, Reader in IT Management at DeMontfort University, put it: "The thing you need to understand is that the technology varies… There are so many factors that mean it's not a homogenous technology. You have to look at the individual suppliers."

What is acknowledged by everyone working in this space is that FR algorithms have improved enormously over the last decade or so, with more improvements likely in the years ahead.

Later in this paper we delve into the debate around accuracy and bias in much more detail. But here it's worth briefly touching on two main studies that we regularly refer to throughout this report.

The first is actually a series of studies from the National Institute of Standards and Technology (NIST) in the USA. NIST produces regular reports comparing and ranking the different FR algorithms available on the market today, with **the most recent results published** this year. Strong performance in these tests is venerated by private suppliers and police users alike.

The second key study is the **2023 report from the National Physical Laboratory (NPL)** on the FR algorithm used by policing in England and Wales. It found promising results in relation to all three types of FR: live, retrospective, and operator-initiated. There are some caveats however, which we'll explore later on.

Setting the standard

Alongside the raw technology, the other major factor is how individual users deploy it. This is where another key term comes into play.

Let's take the NEC Neoface V4 algorithm tested by the NPL last year. Crucially, this analysis looked at the algorithm's performance at different face-match threshold settings. This setting is on a scale from 0 up to 1. And it determines how close a similarity you need between the image you're providing and the one in the database to give a possible match. When the system shows a match, it gives a similarity score – the higher the score, the more likely it is to be the same person.

With the Neoface system, the default threshold is at the 0.6 level. This means the FR system will provide potential matches with a similarity score of 0.6 or above. This isn't a percentage chance though; a similarity score of 0.71 is not the same thing as a 71% chance that it's the same person.

If you lower the threshold, for example down to 0.58 or 0.56, the system will throw up more matches – but it's also more likely to provide a false positive. It lets more options through because there's a lower 'hurdle' to clear for something to count as a potential match.

Conversely, if you increase the threshold to 0.62 or 0.64, it creates a higher 'hurdle' to overcome for an image to register as a match. The system will throw up fewer matches, reducing the risk of false positives, but increasing the risk that you'll miss a genuine match ('a false negative'). So, the threshold you set really does matter.

All of this just scratches the surface of FR. There are plenty more debates, statistics and key terms to come. But this is at least a good place to start. Next we'll turn all of this into something more concrete – looking at a police FR deployment on the ground.

CLICK HERE
Report
MPS LFR deployments 2023-date
Data from the Metropolitan Police on live facial recognition deployments
met.police.uk

CLICK HERE
Report
Face Technology Evaluations - FRTE/FATE
Evaluation of face recognition and analysis technology
nist.gov

CLICK HERE
Report
Facial recognition technology in law enforcement equitability study
Results of an evaluation of facial recognition technology
science.police.uk

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition on deployment

Policing Insight's James Sweetland joined officers and staff from the Metropolitan Police for a live facial recognition deployment, to gain a better understanding of the operational benefits and challenges as well as the public response to this new technology.

We start the day at 10am in West London, outside Ealing Police Station. It is – our press contact says – an "impressively ugly" building and another London police station that's no longer open to the public.

It's Wednesday 3 April and Policing Insight has been invited to attend the Metropolitan Police's latest live facial recognition (LFR) deployment – the first one ever to take place in Ealing. It's an example of how the Met is looking to expand its use of LFR, moving away from the Central London and Croydon deployment locations which have tended to dominate so far.

Pre-deployment briefing

As the Met's Director of Intelligence Lindsey Chiswick – the National Police Chiefs' Council (NPCC) Lead for Facial Recognition – told us in an interview for this project, every LFR deployment begins with a briefing for the officers who will be involved on the day. In Ealing this

> **"Every LFR deployment begins with a briefing for the officers who will be involved on the day... delivered by a member of the Met's small central FR unit."**

is delivered by a member of the Met's small central FR unit, which reports directly to Ms Chiswick. While the material in the briefing itself is confidential, Policing Insight was able to listen in to the 45-minute session.

In the room were Chief Superintendent Sean Wilson (the local borough commander), specialist officers, frontline supervisors, and

Continued overleaf ↘



Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

What is facial recognition?









the group of 'engagement officers' for the day – regular cops who will be stopping those flagged up by the LFR cameras. The briefing is quite comprehensive, covering the basics of how the technology works, common questions from the public, and some of the Met's findings from LFR deployments so far.

Later on, in an exclusive interview with Policing Insight, Ch Supt Wilson tells us: "It's very difficult to cheat live facial recognition. For me, it's a significant step forward in how we do proactive policing across the command. We will always do it with ethics and make sure our policing model is proportionate. And we will do it within the confines and boundaries of the legislation that's available to us."

> **"I would say to any community or any senior politician, if you've got people wandering around in our societies who are very serious, wanted offenders – who have committed some very serious offences – you and I are going to want them taken off the streets."**
>
> **Ch Supt Sean Wilson, Met Police Borough Commander**

On the deployment

With the briefing done, we head down to Ealing Broadway train station, where today's deployment is taking place from midday. The station sees a lot of traffic, with the most recent Transport for London data suggesting 46,395 entries and exits from this station on a typical Tuesday.

The centrepiece of the deployment is a single van parked directly in front of the station, with LFR cameras positioned on the roof. A set of stabilisers are used to raise up part of the van, making sure the cameras are level on this downward-sloping road. As the officers involved are keen to point out, the Met does take measures to make

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

this an 'overt' deployment. There are some bright orange signs on lamposts near the deployment. The force has tweeted that LFR will be used in advance. And the van itself has a sign stating that LFR is in operation, though it's too small to be seen unless you're already on camera – within the so-called 'zone of recognition'.

What's most striking is how many officers are involved on the ground. As well as operators inside the van – those who are shown the matches generated by the LFR system to provide human confirmation – there's the officer who led the morning briefing, with an observer from Bedfordshire Police. Alongside them are around 12 more frontline officers, some next to the station's entrance, some on the other side of the road. It's perhaps the sheer number of officers physically present that's most likely to alert members of the public that something's going on.

And it's these officers who do the public-facing work. If a match is found with someone on the watchlist – which contains individuals the police either want to arrest, or check are complying with legal conditions – they'll stop the person. We're told that this specific watchlist is only for this deployment: it will be deleted at the end of the day.

Public response

The public response is decidedly mixed. The main reaction is that very London type of wordless staring, some level of curiosity, but no evident desire to stop and investigate properly. Others play the LFR at its own game, taking plenty of photos of the van and cameras. Some seem pleasantly surprised to see so many 'bobbies on the beat', especially for a reasonably quiet Wednesday afternoon. And there are a few negative reactions – including one man who walks by, notices the cameras and yells at two officers, "You need public consent!", before carrying on towards the Tube.

To our immense good fortune, within 15 minutes of arriving at Ealing Broadway station, the LFR system serves up a match. The

Continued overleaf ➘

Taking serious offenders 'off the streets'

As part of our behind-the-scenes access to the Met's first-ever LFR deployment in Ealing, Policing Insight's James Sweetland interviewed two senior officers – Chief Superintendent Sean Wilson, Borough Commander for the Met's West Area (which includes Ealing, Hillingdon and Hounslow), and Inspector Crystal Govers – about the operation.

Ch Supt Wilson stated that he saw this as the "first of many" such LFR deployments, with plans for it to become "ingrained into business as usual, whenever we think about operations going forward." This included LFR use at other transport hubs in the future, but also areas with "gang violence, violence around drugs, or high [numbers] of robberies". "This is now one of our most significant tools for being proactive around this, particularly where we know offenders who are wanted are missing but have managed to evade being caught," said Ch Supt Wilson.



Click to view the full interview with Ch Supt Sean Wilson and Insp Crystal Govers discussing the Metropolitan Police LFR deployment in Ealing, London

He also stressed the overt nature of the deployments: "I'm going to be quite open about this with the public. I'm telling them we're going to be using it. For me, it's going to be a deterrent I'll be using across the [West Area.]" Insp Govers pointed to her considerable engagement work with communities prior to the Ealing deployment too.

Responding to some of the concerns people often raise about LFR, Ch Supt Wilson said he was "very comfortable around the accuracy of the technology" and "very confident" that it did not discriminate between people from different communities: "Otherwise, I wouldn't have allowed it to be here." He stressed the importance of compliance with the Human Rights Act, noted that "the arbitrator on LFR is the human in the loop", and explained: "If you're not on the watchlist, all of that data [taken from scanning your face] is deleted."

Overall, Insp Govers described a "massive air of excitement" among officers about LFR. And she expressed remarkable confidence in the tech, saying: "I'm going to go out on a limb. It's a flawless system, I believe, and it has a very good success rate." Ch Supt Wilson concluded with a more measured, but direct appeal to what LFR can do. "I would say to any community or any senior politician, if you've got people wandering around in our societies who are very serious, wanted offenders – who have committed some very serious offences – you and I are going to want them taken off the streets."

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

What is facial recognition?

engagement officers receive an audible 'ping' on the mobile devices they've been supplied with. The two nearest police officers move towards the target. It's a white male. He's generally compliant, though appears agitated at some points. The officers engage in a long conversation with him; later, the deployment leader also speaks to the man.

Eventually, perhaps 20 minutes on, they allow the man to continue on his way. Given that this was confirmed to us as a 'true positive', our assumption is that he wasn't wanted for arrest, but for the police to check he's complying with whatever legal conditions have been applied to him.

Ultimately, it is no different to many standard police stops. The officers engage calmly with the person, conduct whatever checks they need, and then send him on his way. Yet behind it is this new system of LFR, one that the **Met claims** is a breakthrough in crime-fighting on the scale of DNA. In the end, the **Met's records** show that this first Ealing deployment lasted six hours and 11 minutes, scanning around 2,500 faces. It yielded no false alerts – none of those 'false positives' previously mentioned – and four confirmed matches.

The four positive alerts didn't lead to any arrests. They are instead listed as "no action" in the Met deployment record. This implies that each stop was to check people were following legal conditions, rather than, for example, outstanding warrants for arrest. The police would also argue that an LFR deployment can deter criminals from visiting the area, and provide public reassurance.

CLICK HERE
Article
How facial recognition technology has changed policing
Scanning tool is the biggest game-changer for officers since DNA, says Met's intelligence director
thetimes.co.uk

CLICK HERE
Report
MPS LFR deployments 2023-date
Data from the Metropolitan Police on live facial recognition deployments
met.police.uk









Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Outside the police: how the private sector is using FR

While growth in the police use of facial recognition has been subject to considerable scrutiny and calls for transparency, use in the private sector has in some cases gone further and faster.



One striking feature of the global debate about facial recognition (FR) is how, in many jurisdictions across the world, the private sector has gone further and faster than law enforcement – and not just the well-established, relatively uncontroversial examples, such as facial ID to unlock your phone, but the use of live facial recognition (LFR) for public safety purposes.

This is perhaps most obvious in the retail space, where private companies have turned to LFR to help them deal with theft and other crime in their stores. It's something that's caught the interest of regulators, with a range of outcomes – from **ongoing inquiries in New Zealand** and critical findings in **the Netherlands** and **Canada**, all the way to a **more positive finding** by the UK's Information Commissioner's Office in relation to the company Facewatch.

Inside the Facewatch scheme

Policing Insight spoke to Facewatch's CEO, Nick Fisher, to understand how its retail LFR scheme works. He explained: "We trialled it with the [supermarket chain] Southern Co-Op, they were our first big customer. But we're nationally covered now, with about 1,000 plus stores in the UK using Facewatch.

"The police don't have the resources to deal with low-level [retail] crime, but often these days that comes with violence and aggression too. So, [I thought], let's come up with a solution that deters and prevents the horrible guys from going into stores. That's what we did. The model was to commoditise FR so it's affordable for retailers who want to take it."

Facewatch told Policing Insight that it has an exclusive agreement with the company Real Networks to use its SAFR algorithm. And Mr Fisher stated that Facewatch has repeatedly shifted to use the best algorithms available: "We've changed our algorithm five times. This is the best algorithm, the most accurate with the best dataset, that we've ever used. We've been going with SAFR for just over two years."

The company's Director for Privacy, Dave Sumner, explained how the system works in practice. If someone commits their first ever retail offence in a store that uses Facewatch, the retailer reports the crime – sharing details and any suspect photos taken from in-store cameras – with the company. This report is "then screened by ex-police officers to make sure it actually amounts to a crime". If it does, the suspect's image is placed on Facewatch's database.

> **"The police don't have the resources to deal with low-level [retail] crime, but often these days that comes with violence and aggression too. So, [I thought], let's come up with a solution that deters and prevents the horrible guys from going into stores. That's what we did."**
>
> **Nick Fisher, CEO of Facewatch**

The LFR comes into play if someone on this database enters a Facewatch-equipped store again. If their face is identified by the store's LFR camera, "an alert is sent to a mobile device that we've supplied to them," continued Mr Sumner. "It will show the image that's just been captured by the Facewatch camera somewhere in the store and up to six accompanying 'gallery images' of the same person. The store's job is to press 'match' or 'no match' (this lets us audit the data we send out). They then have a chance to intervene before a crime has happened."

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

What is facial recognition?

Some are highly sceptical, however. In its May 2023 report ***Biometric Britain***, the campaign group Big Brother Watch – long critical of Facewatch – wrote: "The use of LFR in retail environments is a deeply concerning development… 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."

The same group are supporting a **legal challenge** brought by a woman who claims she was misidentified by the Facewatch system. She described what happens as follows: "I was visiting Home Bargains and had only just got into the entrance of the store when a member of staff came up to me and told me I had to leave the store immediately because I was a thief. I had my bag searched and was escorted out of the shop, and was told due to facial recognition I was banned from shops across the whole country."

"I have never stolen in my life and so I was confused, upset and humiliated to be labelled as a criminal in front of a whole shop of people."

There's also evidence that the public are much more wary of retailers using FR than they are of law enforcement doing this. A **March 2024 report** from the Alan Turing Institute found that 79% of UK citizens trust police forces to use biometric systems, compared to just 38% when it comes to retailers. And only 45% of people said they were 'comfortable' with retailers using biometrics to identify suspects linked to shoplifting or violence.

Private policing?

It's notable how much Facewatch operates like a police organisation. The company takes crime reports from subscribers, checks them with ex-police officers, and then builds a database of suspects. Mr Sumner himself is formerly of West Midlands Police. In fact, he told us, he has "sufficient staff to manage more reports of crime than West Midlands Police". "We are the UK's second largest police force for the volume of incidents of retail crime that we record," he added.

Facewatch doesn't give every store access to every face on the database. Instead, akin to a policing service again, it undertakes crime analysis so that the highest-risk offenders are available nationally, but low-risk offenders are only included locally. Mr Sumner said: "I've looked at academic data on offending patterns, what different offender cohorts do, whether they're opportunist, prolific, etc. I've based the sharing radius on that information to ensure it's not a sledgehammer to crack a nut. It's proportionate to the offence."

> **"The Policing Minister is telling shops: 'Just install your own private surveillance system, that's what's going to stop this massive problem with violent shoplifting.' It's really insulting to people who work in those situations; it's a total acknowledgement that the basics of policing aren't being done adequately and it's putting everyone at risk."**
>
> **Madeleine Stone, Big Brother Watch**

There have been other FR efforts on the retail crime front in England and Wales. There's **Project Pegasus**, a new £840,000 initiative in which 13 retailers are paying policing to run CCTV images against faces in the Police National Database using retrospective facial recognition (RFR). And the UK Government has announced a new **£55.5 million Home Office investment in FR** to help tackle retail crime, including £4 million for mobile LFR units.

In an interview with Policing Insight, Big Brother Watch's Senior Advocacy Officer, Madeleine Stone added that this use of LFR is "an acknowledgement of failings within the policing system".

She said: "The Policing Minister is telling shops: 'Just install your own private surveillance system, that's what's going to stop this massive problem with violent shoplifting.' It's really insulting to people who work in those situations; it's a total acknowledgement that the basics of policing aren't being done adequately and it's putting everyone at risk."

This type of private use isn't confined to the UK. Phil Thomson, CEO of Auror, told Policing Insight that his company has long tried to help retailers (particularly in Australia and New Zealand) work with the police. "After an event has occurred, that security guard or store manager would report what occurred into the Auror platform. We help them with that entire reporting process and gather the evidence (which could be witness statements, receipts, video footage) and capture all that in one place. They could then provide it to the police with a click of a button."

The company has also recently expanded into using RFR – "image matching after the fact" – to help identify suspects committing crimes. While the company "doesn't do LFR or cameras at all in stores", Mr Thomson said, it has enabled retailers to use RFR in five countries so far: the UK, US, Australia, New Zealand, and Canada.

As we'll show throughout this report, the use of LFR has taken off in supermarkets worldwide – including a major trial by the **Foodstuffs co-operative chain in New Zealand** – and in many cases, this is outmatching what the police appear to be doing.

Stadia, casinos, factories and more

Outside the retail sector, FR is now regularly used in many stadia and venues globally for public safety purposes. That includes one astonishingly early deployment of LFR at the 35th Super Bowl in 2001 – something we'll cover later on in this report.

But there are plenty of other examples too. **An extensive report published by the US National Academies of Sciences, Engineering and Medicine** earlier this year includes several of

Continued overleaf ➘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

What is facial recognition?

them. It describes FR as "commonplace" in sports venues and claims that: "The systems used for Taylor Swift have been effective in keeping the artist safe from… [her] approximately 3,000 known stalkers, many of whom attend her shows." Plenty more venues, **including several in Australia**, have also begun using LFR.

The National Academies' report also points to a much more controversial example of LFR: "Madison Square Garden and Radio City Music have been reported to use facial recognition technology (FRT) to identify lawyers who work at firms with pending litigation against them. Lawyers have reported being escorted out of the venue, despite having purchased tickets and having never been involved in litigation against these venues." This use of FR to enforce an "attorney exclusion list" (a term **reported by the *New York Times***) seems difficult to justify.

"Many casinos", the same report continues, "along the Las Vegas strip, and elsewhere in the United States, have implemented FRT to supplement security and monitor prohibited activity, allowing for real-time identification of individuals who were previously barred from gaming establishments to be blocked or removed." The Japanese company NEC, which supplies the algorithms used by British police forces, told us that it too has provided FR capabilities to eight casino venues in the US, Australia, and New Zealand.

And there are plenty more examples. The use of FR to verify identity at borders, especially in airports, is now more-or-less ubiquitous in some countries. **FR is being used to verify access to some buildings**. One industry publication has **described** its use in Toyota factories, "to confirm with high-speed and accuracy that the person working on and inspecting different parts of the car manufacturing process are the right ones, ie, the wheel technician is on the wheel assembly while the engine technician is on the engine line."

The private sector's use of FR – whether live or retrospective – for crime prevention, public safety or safety-adjacent purposes is increasingly evident, taking place in locations from supermarkets to stadia. Throughout this report, we'll explore how some of these key examples have helped to shape the debate around law enforcement use.



CLICK HERE
Article
Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology
Supermarket wanted to switch its FR system back on
edpb.europa.eu

CLICK HERE
Report
Blog: Balancing people's privacy rights with the need to prevent crime
Considerations around LFR use in the retail sector
ico.org.uk

CLICK HERE
Report
Biometric Britain: The Expansion of Facial Recognition Surveillance
Civil liberties campaign group investigation of FR use in the UK
bigbrotherwatch.org.uk

CLICK HERE
Report
The Future of Biometric Technology for Policing and Law Enforcement
Exploring the future of biometric technology for UK policing
cetas.turing.ac.uk

CLICK HERE
Article
Action plan to tackle shoplifting launched
The government brought together retailers and policing to set out measures to tackle the rise in shoplifting
gov.uk

CLICK HERE
Report
Facial Recognition Technology
Current Capabilities, Future Prospects, and Governance
nap.nationalacademies.org

CLICK HERE
Article
Facial recognition technology in use at major Australian stadiums
Biometric data is being collected by stadiums
choice.com.au

CLICK HERE
Article
Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies
FR used to keep people out of concerts and sporting events
nytimes.com

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

The future of facial recognition

Rapid improvements in FR technology and more widescale adoption are driving the sector forward, but it is also important to consider how existing resources could be applied in new ways and what the next generation of biometric technology might look like.



The scale of activity around facial recognition (FR) is vast. From live facial recognition (LFR) in England and Wales and many retail spaces worldwide, to retrospective facial recognition (RFR) use by police across the globe, it's already part of our everyday reality.

At the same time, the algorithms underpinning FR have improved rapidly in recent years. They're much more accurate and can increasingly make identifications in challenging conditions – FR that can handle masked faces is an example of this – so things are clearly changing, and changing fast. Against that backdrop, it's important to consider how existing FR could be applied in new ways, and what the next generation of biometric tech might look like.

Body-worn FR

Body-worn video cameras are a ubiquitous technological development in policing. For officers around the world, they're increasingly accepted as a standard part of their kit. As yet, police in England and Wales haven't used LFR within body-worn cameras. But UK Chief Scientific Adviser for Policing, Professor Paul Taylor, told Policing Insight: "It's interesting because the technology is there. There are body-worn cameras you can buy that have FR built in. They're used overseas in areas where you would not have a good Wi-Fi signal. But, for me, I think this [application] is on a more than five year time-horizon."

However, that longer-term timeline is because of the practicalities rather than the tech: "Let's say I put a watchlist of outstanding serious sexual offenders on the body-worn camera and it buzzes [when someone is identified]," continued Prof Taylor. "Does the officer arrest them? Do they even know who it buzzed for? There are some complications in making it a 'live system' which need to be

Continued overleaf ➘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

worked through. Yes, the tech's there, but the governance and the systems to work it through are a bit more complicated."

The NPCC Lead for FR and Met Police Director of Intelligence, Lindsey Chiswick, expressed a similar view: "We've seen some other opportunities around, such as Southampton [security guards] who've been trialling body-worn video. I don't know about that. I'm a bit lukewarm, but I'm quite interested to see how it pans out."

As **Policing Insight reported in March**, tech company Reveal Media is indeed running a trial of LFR-equipped body-worn cameras in Southampton night-time venues. Although relatively small scale – it involves an 'exclusion list' of 65 people, just six cameras, and had only 10 hits in its first nine weeks – it shows what's already possible and what policing could do in the future. Other vendors, such as Motorola, also have FR-enabled body cameras of this kind.

Drones and CCTV

Another possibility is the deployment of FR-enabled drones, most likely in the context of large-scale public events. Prof Taylor explained: "That's probably a little bit closer, potentially, for big events where you're trying to spot known criminals… I could see the case for using drone footage where we need to protect the crowd because a group of individuals are there to commit harm. It [offers] a quick way to establish where those [people] are… that would then be fed back to officers on the ground to prevent crime from happening."

> **"I could see the case for using drone footage where we need to protect the crowd because a group of individuals are there to commit harm. It [offers] a quick way to establish where those [people] are… that would then be fed back to officers on the ground to prevent crime from happening."**
>
> **Prof Paul Taylor, UK Chief Scientific Adviser for Policing**

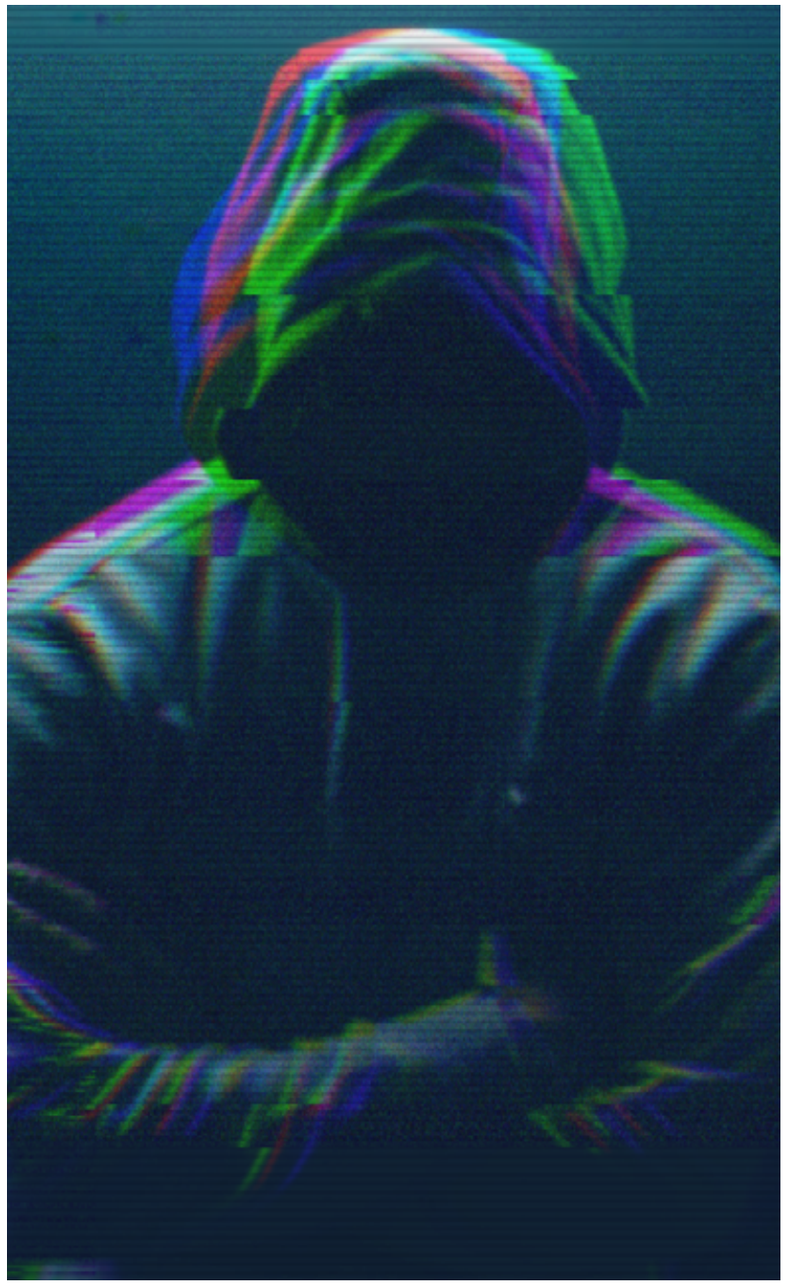
Could it be on the way in the UK? "The technology is definitely within reach," said Prof Taylor. "Though where the Americans have it, it's difficult to disentangle the LFR part from the general use of drones. I've seen examples where they've spotted the person they want, and from the drone footage were able to establish that they weren't actually carrying a real firearm, but a replica instead." He added: "It's an interesting opportunity, but we have no plans currently to do it."

Beyond that, a more advanced and controversial example would be embedding LFR into CCTV networks. This has already been done in some places, most famously throughout China, but also in **Moscow**. Prof Taylor offered a more cautious verdict on this potential development: "With hooking into CCTV systems, I think there has to be a lot of thought and consideration before we do that, particularly when it comes to LFR."

The UK's Biometrics and Surveillance Camera Commissioner, Tony Eastaugh, hinted at the same dangers. "The default position is that we're the second most surveilled society in the world. I think we've always accepted that, because the position of the UK and our citizens is: 'The government and the authorities are here to protect us.' But, as time goes on and people start to understand more about how FR could be used against them in different formats, I think we're going to get some very difficult questions back from the public."

There are also practical challenges to relying on CCTV in some countries, as one example from Dr Andrew Chen, Senior Research Fellow at Koi Tū (the Centre for Informed Futures) at the University of Auckland, revealed. "In New Zealand, the cameras we have access to in major cities are actually owned by transport agencies and their primary function is to monitor traffic.

"One of the funny things is that if there's a pan, tilt or zoom functionality, the person on the police side can move the camera to try and watch something, but the transport office has ultimate control. So they can just move it back, saying: 'Sorry police, we need that right now.'"



Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Though all these potential uses differ, they should generally be covered by existing UK regulation. As Emily Keaney, Deputy Commissioner for Regulatory Policy at the UK Information Commissioner's Office put it: "We would always encourage organisations to ensure they are thinking about how they bake in data protection by default, and this will be particularly important to consider as new use cases emerge. But generally, we're still talking about the same fundamental principles around data protection. While the technology may evolve it's still the same rule book."

Inferential tech

Beyond these fresh applications of FR, there are some more futuristic and novel opportunities which look likely to provoke public debate. One FR-adjacent example is set to be rolled out in France during this year's Olympic Games. **According to Reuters**, this new 'AI-powered surveillance' works not by identifying faces on video streams, but by spotting specific actions. This includes "crowd surges; abnormally heavy crowds; abandoned objects; presence or use of weapons; a person on the ground; a fire breaking out; contravention of rules on traffic direction". A **similar example has been publicised** by US company Abto Software.

While some of these systems deliberately eschew facial-matching, others seek to go even deeper – not just identifying faces, but trying to read emotional or psychological states from them. For example, US firm **Affectiva AI claims** it's collected an enormous database, including 14.7 million face videos from 90 countries, and has used this data to train AI which can detect emotional states from people's facial expressions.

These so-called 'inferential systems' are highly controversial. A recent **Alan Turing Institute study** suggested that while 60% of UK citizens are 'comfortable' with police and law enforcement use of 'identification biometrics' like FR, this drops to just 29% for inferential tools – which also includes things like polygraphs (another topic **Policing Insight has covered**). The report adds:

> **"We would always encourage organisations to ensure they are thinking about how they bake in data protection by default, and this will be particularly important to consider as new use cases emerge. But generally, we're still talking about the same fundamental principles around data protection. While the technology may evolve it's still the same rule book."**
>
> **Emily Keaney, UK Information Commissioner's Office**

"Behavioural inferences (such as detecting emotions) are likely to be highly unreliable due to a lack of scientific validity in research of inferential systems."

And there are further categories of biometric systems in development, **according to the same study**. This includes 'gait analysis', where AI is used to evaluate how a person moves. This could help spot if someone's carrying a weapon or even provide a novel way of identifying them. If an AI system can capture the unique way someone moves, could it be used to spot them the next time they walk past a camera?

There's also discussion of 'gaze estimation', a biometric approach which can analyse what someone is looking at. This could "be used to monitor individual behaviour considered to be suspicious – for instance to detect whether they are conducting hostile reconnaissance".

Preparing for the future

In some ways, these more advanced tools are beyond the scope of this report; we're focusing exclusively on FR, which offers more than enough to talk about.

But, when exploring the opportunities offered by FR, it's important to take these next-gen technologies into consideration. As Tony Eastaugh noted, the choices we make around FR now will set the stage for how we regulate future tech too: "The next generation of – I was going to say cameras, but they're really sensors – could be far more accurate. They might not actually rely on the biometric 'ones and zeros' of your face at all. They will go on your body odour or how you walk. They will go on whether you're more likely to be in Croydon town centre at 2pm on Thursday or 5pm on Thursday: that big data which crunches down to apply theories or intents to people's movements.

From a strategic perspective, the question we've got to keep asking ourselves is: 'Are our processes and frameworks keeping track with the speed of technological advances?' The stuff we've put in place today – the mitigations, the frameworks, the accountability, the scrutiny – is that fit for tomorrow, bearing in mind the advances that are already taking place?"

CLICK HERE
Article
Door staff equipped with body-worn facial recognition cameras identify offenders in city centre trial
Details of a three-month facial recognition trial in Southampton
policinginsight.com

CLICK HERE
Article
Russia Is Building One of the World's Largest Facial Recognition Networks
It may even be bigger than China's 200 million camera system
themoscowtimes.com

CLICK HERE
Article
How France plans to use AI surveillance to keep Paris 2024 Olympics safe
France tested AI-driven video surveillance technology
reuters.com

CLICK HERE
Report
The Future of Biometric Technology for Policing and Law Enforcement
Exploring the future of biometric technology for UK policing
cetas.turing.ac.uk

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

2

Facial recognition around the world

Facial recognition around the world Stakeholder voices



"We devised five key vulnerability factors… which help you come up with a 'moderate', 'significant' or 'extreme' determination of how people's rights are being impacted. If it's being used by police, it's going to hit our 'extreme' risk level and, in normal circumstances, we recommend it should be banned."

Lauren Perry
Policy Specialist at the Human Technology Institute, University of Technology Sydney

"We've long said FR is a fundamental violation of people's rights and shouldn't be allowed in any format. And if it's allowed in the EU, there can also be a knock-on effect across the rest of the world."

Ella Jakubowska
Head of Policy, European Digital Rights Network





"There's just no 'social licence' for LFR in New Zealand; it's highly, highly controversial… I think there would be very little acceptance of police doing it in a live setting, in the way that maybe it's been done in the UK.

Dr Andrew Chen
Senior Research Fellow, University of Auckland

"The thing that stands out most in England and Wales is that the police are 'bold' compared to other countries in trying the tech. Campaign groups and others consider the UK an outlier in the democratic world."

Dr Asress Gikay
Senior Lecturer in AI, Disruptive Innovation, and Law, Brunel Law School



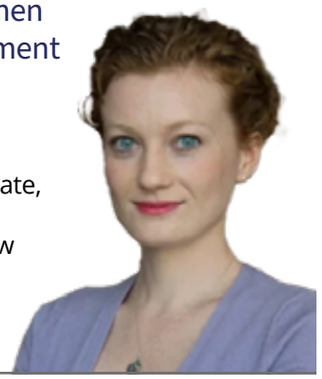
"We're interested in what the UK is doing with LFR… but that's a no-go for us because of the limitations emerging in the EU AI Act. We're fully focused on post-event evaluations in the Dutch Police."



Chief Inspector John Riemen
Dutch Police Lead Specialist on Biometrics

"One of the biggest challenges with understanding how widespread it is in the US is the complete lack of transparency. Agencies aren't forthcoming about which systems they purchase and how and when they implement them."

Prof Clare Garvie
Senior Associate, Georgetown University Law Center





"The political will and ambition is to increase the number of cameras and [explore] the possibility of using LFR… The political pressure is strong to make it even easier for law enforcement to use powerful surveillance technology, such as LFR, in the near future."

Marie Eneman
Associate Professor in Informatics, University of Gothenburg



"As far as we're aware, we haven't seen any proposals for building up an FR database. Our understanding is that it's investigation-specific and limited use cases, but again we'd want to see that either in the Bill or in the future Code of Practice."

David Murphy
Assistant Commissioner, Irish Data Protection Commission

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

England and Wales: world leader or global outlier?

England and Wales have two of the most advanced implementations of facial recognition for policing in the Western world. To some, that is a cause for celebration, but for privacy campaigners it's a warning that the police have gone too far.

England and Wales is the most advanced jurisdiction in its policing use of facial recognition (FR) in the Western world. Live facial recognition (LFR) is widely used and its use is set to grow in the near term. For that reason, we'll focus on LFR in England and Wales, before touching more briefly on retrospective facial recognition (RFR) and operator-initiated FR (OIFR) later on in this detailed piece.

According to Dr Asress Gikay, Senior Lecturer in AI, Disruptive Innovation, and Law at Brunel Law School, "the thing that stands out most [in England and Wales] is that the police are 'bold' compared to other countries in trying the tech". He continued: "Campaign groups and others consider the UK an outlier in the democratic world. They're partly right in that other parts of the world, especially the EU, aren't currently using it. In that sense, the UK is an outlier."

Statistics & facts

105	the total number of LFR deployments by the Metropolitan Police since 2020
115	the number of LFR deployments by South Wales Police since 2017
0.64	the face-match threshold now used by South Wales Police
86%	proportion of Britons who believe FR in policing would be either 'very' or 'somewhat' beneficial
£4m	pledged by the UK Government over the next four years to fund "bespoke mobile units" with LFR capabilities to be deployed to high streets

The supporters of the police use of LFR, who include **UK Policing Minister Chris Philp**, argue that the progress made in England and Wales makes us a world leader. For those opposed, it makes us a global outlier among Western states.

The use of LFR is now most commonly associated with the Met and South Wales Police, but it's often forgotten that Leicestershire Police got there first. In 2015, this force deployed LFR at the Download festival, the first time it had been used in England and Wales. The police scanned 90,000 faces which were "checked against a Europol watchlist… [with] captured images deleted afterwards", according to **one academic paper**. The same force had also taken some of the first steps to deploy RFR, based on **reporting** in 2014.

But while **Leicestershire, South Yorkshire, Greater Manchester and Humberside Police all ran their own brief trials** (six months or less) between 2015 and 2018, South Wales and the Met quickly became the main users of LFR, with their own trials lasting for several years.

The Met's website contains **combined data on all its LFR deployments**, although it appears to no longer contain records pre-2020. However, an **independent report** from Professor Peter Fussey and Dr Daragh Murray on the Met's early trials reveals some of the controversial decisions made by the force.

Its first two LFR test deployments – in August 2016 and 2017 – both took place at the Notting Hill Carnival, an event often marked by tension between the police and the Black community, and potentially a high-risk choice for trialling new tech. As Fraser Sampson, Professor in Governance and National Security, Sheffield Hallam University, put it: "The early deployments that

Continued overleaf ➘



took place, both in the UK and in parts of the US, were like if you made a list of the very places that you wouldn't test LFR. Notting Hill Carnival is probably up there in the top five. Why wouldn't you try it in a setting where you've already got enormous support and understanding from the community?"

Other early deployments took place in central London's Soho district, and in Stratford and Romford in the east of the city. Some data on these was published by the Met and the National Physical Laboratory in a **separate report** back in 2020.

South Wales Police publishes all of its deployment data (from 2017 onwards) in **one place**, including a number of early trials at Cardiff's Millennium Stadium. It shows that the force's very first LFR use was at the venue during operations for the Champions League Final. Juventus were well beaten, losing a fifth final in a row. The LFR system didn't perform much better; of 2,632 alerts, 2,554 were incorrect, meaning just 8% of the total hits were accurate.

Although no other early deployments saw anywhere near as many false alerts and things did improve across the year, it wasn't an isolated event. An Anthony Joshua boxing match in October 2017 saw 51 alerts, with 46 incorrect; a Wales v Italy game in March 2018 saw 23 alerts, all of which were incorrect. While other events were much more successful – a Liam Gallagher concert generated six alerts, all accurate – it's fair to say that many of these early trials had decidedly mixed results.

Unsurprisingly, these trials attracted some criticism. The **academic report** by Prof Fussey and Dr Murray argued that it was "highly possible that the LFR trial process adopted by the [Met] would be held unlawful if challenged" in court. Another **report from the Minderoo Centre** suggested: "These deployments [including both the Met and South Wales] did not incorporate many of the known practices for the safe and ethical use of large-scale data systems." And campaign group Big Brother Watch **called** the growth of LFR an "unprecedented threat to citizens' privacy and civil liberties".

The Bridges case

The next major LFR development in England and Wales involved a landmark case brought against South Wales Police by a man named Ed Bridges. It was supported by human rights group Liberty and is widely regarded as the first legal challenge to LFR use in the Western world.

It began, **Mr Bridges told BBC News**, when he was caught on an LFR camera in December 2017: "I popped out of the office to do a bit of Christmas shopping and on the main pedestrian shopping street in Cardiff, there was a police van. By the time I was close enough to see the words 'automatic facial recognition' on the van, I had already had my data captured by it. That struck me as quite a fundamental invasion of my privacy."

> **"I popped out of the office to do a bit of Christmas shopping and on the main pedestrian shopping street in Cardiff, there was a police van. By the time I was close enough to see the words 'automatic facial recognition' on the van, I had already had my data captured by it. That struck me as quite a fundamental invasion of my privacy."**
>
> **Ed Bridges, legal challenger to South Wales Police**

His legal challenge to South Wales Police covered several areas, as set out in the **skeleton argument** presented before his High Court hearing in 2019. While Mr Bridges did "not suggest that the Defendant or other police forces could never lawfully deploy" LFR, he raised concerns about violation of privacy rights, data protection and equality legislation in the current approach.

In September 2019, the High Court rejected his case in each of these areas – a win for the police. But the story didn't end there. Mr Bridges and Liberty challenged the High Court verdict, meaning the Court of Appeal would consider it; and in August 2020, this court reached a rather different verdict – a unanimous decision that accepted three of Mr Bridges' legal arguments. The police stated that they would not contest this decision, and civil liberties groups celebrated a major victory.

A **useful summary of the Court's findings** by Matthew Ryder KC and Jessica Jones in August 2020 sets out the three areas in which the use of LFR by South Wales Police was found to be unlawful. There were "fundamental deficiencies with the legal framework", the data protection impact assessment was flawed, and the force hadn't taken steps to check that the software was unbiased.

Northumbria University Professor of Law, Marion Oswald, gave Policing Insight her sense of what this case meant: "[Bridges] specifically said that the legal basis at the time was inadequate," she explained. "The police have amended their policies to try and deal with the issues the court [found]… But there's no definitive conclusion on whether everything's fine now. It would need another court case to decide if what's been done has satisfied the issues Bridges identified."

The exact interpretation of the Bridges case was a source of considerable debate among those we interviewed. But at the very least, everyone agrees that it gave a nuanced verdict. The Court didn't decide that police LFR was intrinsically unlawful. It also didn't offer anything close to a clean bill of health. It left much to be resolved and plenty of remedial work for the police to do.

After Bridges

The intervening years saw LFR more or less off the table as a policing tactic, partly due to Bridges and also because of the pandemic. In South Wales, **force data** shows that there were no deployments from February 2020 to February 2022. In 2022, LFR was used just twice. There was then another lengthy gap, with the next deployment only coming in May 2023. But since then, its use has become much more frequent.

It was largely **the same picture for the Met**. From March 2020 to December 2021, no LFR was used; in 2022, it was deployed six times (in

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition around the world

January, March and four occasions in July) and then as in South Wales, there was a lengthy gap until April 2023. However, LFR is **now regularly used by the Met**, including many deployments in Croydon (an area partly represented in Parliament by Policing Minister Chris Philp) as well as others in central London and beyond.

For an understanding of how police use LFR at an operational level, turn to the 'on-the-ground report' of a Met deployment in the first chapter of this paper. But there are now some standard key principles in place. Both the Met and South Wales tend to publicise deployments, whether posting about them on social media (or websites) in advance, or placing physical signs just outside the LFR camera's 'zone of recognition'. They use watchlists of varying sizes, which include people wanted for arrest, those who've not turned up at court, and others the police want to check are complying with legal conditions (such as sex offenders).



The cameras scan every face that goes by; images flagged as a match are referred to human operators for confirmation, before officers engage the individual involved. For scanned faces that don't match, the data is instantaneously deleted.

The police argue that LFR offers serious benefits. In February, Met Director of Intelligence and NPCC Lead for Facial Recognition Lindsey Chiswick told us: "In Croydon, we've deployed eight times this year and made 64 arrests. Each deployment has 12-18 officers. If you took the same 12-18 uniformed officers on the street without that tech, they'd have nothing like the success the [LFR] has." The Policing Minister previously **told Policing Insight** about someone wanted for GBH since 2015 who was also recently caught by LFR.

> **"We've deployed eight times this year and made 64 arrests. Each deployment has 12-18 officers. If you took the same 12-18 uniformed officers on the street without that tech, they'd have nothing like the success the [LFR] has."**
>
> **Lindsey Chiswick, Met Police Director of Intelligence, and NPCC Lead on Facial Recognition**

The UK Chief Scientific Adviser for Policing, Professor Paul Taylor, agreed, adding that the public sometimes have "a lack of awareness of just how effective LFR has been in arresting some of the worst people in society"; he also spoke about its deterrent effect. And South Wales former Police and Crime Commissioner Alun Michael told us, "the point with LFR is to recognise it as a preventative measure", citing examples such as the potential to catch paedophiles in the vicinity of music concerts attended by many young girls.

New guidance and new studies

Since the Bridges case there's been an effort by policing to address some of the key concerns raised. "The big thing that's different", according to Ms Chiswick, is "the College of Policing's authorised professional practice (APP)". She said that although not law, "it's a code policing is expected to follow" when it deploys LFR – essentially formalised guidance for all forces across England and Wales.

Originally published in 2022, the **APP** covers a wide range of areas around LFR: human rights, data protection issues, criteria for deployment, constructing and using watchlists, performance metrics, legal context and more. It's intended to give a framework to address some of the deficiencies highlighted in the Bridges case.

And on the specific legal basis for LFR, both **the Met** and **South Wales Police** have published 'legal mandate' documents setting out their approach. There are also much more detailed standard operating procedures produced by each force. Despite this, it's notable that there is some consensus that the legal basis remains very complicated, regardless of the view on FR. Dr Asress Gikay, an academic supportive of police LFR, called it "admittedly, complex". Both Lindsey Chiswick and Madeleine Stone (Senior Advocacy Officer at Big Brother Watch) referred to it as a "patchwork" in interviews, and there's a robust debate over whether a single piece of legislation is needed (as we'll explore in the next chapter).

In addition to the College APP, the **National Physical Laboratory (NPL) report** published in March 2023 is an 'equitability study' which looked at the potential bias in the NEC Neoface V4 algorithm used in LFR deployments by the Met and South Wales Police. It was much-trumpeted by the police, as **Policing Insight reported**, and it's easy

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

to understand why. The independent evaluation of LFR in "typical operational conditions" found that, when a 0.6 face-match threshold is used, there is "no statistically significant" bias. The Met has stuck to this level in all LFR deployments, while South Wales uses an even more exacting standard (0.64).

While the debate around disproportionality and bias remains (and is something we explore in more detail later in this report), the NPL study offers at least some effort to address Bridges too.

No consensus yet

Of course, these changes have not fully reassured or convinced everyone. Andy George, President of the National Black Police Association, told Policing Insight he supports a "pause for a short period" in the police use of LFR. He continued: "We need to have a consultation with the community, with human rights groups like Liberty, Amnesty and others. We need to have that debate. We then need to come up with that ethical framework of what we're going to do and push on from there."

Madeleine Stone added that Big Brother Watch's position is unchanged: "It's a mass surveillance tool that turns the streets of Britain into police line-ups and our faces into barcodes… The fact that every single person has their sensitive biometric data scanned and processed as an ID check is completely disproportionate. We see no way that it could ever be used in a proportionate way."

> **"In five years we'll have a national cadre of vans housed in strategic locations across the country and brought out to keep people safe at major events. They'll be used as an intelligence tool to support areas where they're needed."**
>
> **Prof Paul Taylor, UK Chief Scientific Adviser for Policing**

In October 2023, Big Brother Watch co-ordinated a cross-party campaign where 65 parliamentarians (including Tory MP David Davis, Liberal Democrat Leader Sir Ed Davey, Green MP Caroline Lucas and Labour peer Shami Chakrabarti) joined 31 rights groups in calling for an end to LFR use by police and private firms.

And yet, polling shows the public take a less critical view. **A 2024 Alan Turing Institute study** found that 60% of Britons are comfortable with use of biometric tech to identify criminal suspects in high-diversity, crowded areas. Only 5% wanted biometrics banned in this use case. That appears to follow other data. In November 2022, the same organisation **conducted polling** which found that 86% of Britons believed FR in policing would be either 'very' or 'somewhat' beneficial.

A national cadre of LFR vans?

Either way, the police are set to significantly scale up the use of LFR. So, while there have already been 105 deployments by the Met since 2020 and 115 by South Wales Police since 2017, these numbers are set to keep growing.

Post-pandemic use of the technology has expanded in a limited way to Northamptonshire (at **Silverstone's British Grand Prix**) and Essex Police. In both cases, this was facilitated by 'mutual aid', with South Wales Police providing the tech and guiding new forces in how to use it.

And there is wider interest. South Wales Police Inspector Karl Roberts, currently supporting the National Biometrics Function, told us: "Seven further forces [ie excluding the Met, Northamptonsire and Essex] are currently exploring whether they could utilise LFR, via mutual aid from South Wales." That could mean 11 forces (more than 25% of the total in England and Wales) already making plans to adopt LFR in the coming months.

Despite this, it's worth acknowledging how limited the police's LFR resources are. Ms Chiswick told us the Met has "two vans at the moment – and they double up as CCTV vans too, so we don't have loads of kit". South Wales' fleet is unlikely to be vast either.



In his interview with Policing Insight, Prof Taylor shared his expectations of how LFR usage might change: "My instinct is that, over the next 12 months or so, you'll see more mutual aid and more uses of the current vans. Then there could be potential investment in more equipment and people by forces or nationally, to put vans in strategic locations around the country – big cities that can then support the local region.

"I think in five years we'll have a national cadre of vans housed in strategic locations across the country and brought out to keep people safe at major events. They'll be used as an intelligence tool to support areas where they're needed. We've got the Met deploying roughly twice a week. I think that's not a bad metric to keep in your head. If we had, say, eight vans across the country, deploying twice a week each, that's what I would imagine in five years time."

World leader or global outlier?

Since that conversation, the UK Government has announced its '**retail crime crackdown**', promising £4 million over the next four years for "bespoke mobile units that can be deployed to high streets across the country with LFR [capabilities]". There has also been

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition around the world

repeated briefings to the media about a new strategy. ***The Times* recently stated**: "A Whitehall source said that [LFR] had been so successful that the Government was planning to make a policy statement setting out its facial recognition strategy in May or June." With the Prime Minister deciding to launch a General Election, that strategy's been paused and – given how little we know about Labour's policy (as the likeliest party to form the next government) – it's not clear whether it will ever see the light of day.

There is also ongoing use of FR in other formats. RFR, which compares two images together outside of real-time, is widely used by British policing. Every force in England and Wales can use RFR to search for suspects via the Police National Database which **holds at least 2 billion records** from 220 databases. Some individual forces also use RFR to search within their own records, the Met being one example – a "limited" product **went live in August 2023**.

There's also been a series of limited trials of OIFR in a few police forces. This involves officers using a mobile app to photograph someone, and running the image through a custody database for ID purposes at the scene. It's not strictly live, but it's barely retrospective either – 'near-live' might be a good summary.

Inspector Karl Roberts explained that OIFR is used in cases where "someone is refusing to or can't provide their details". "It could be that they're unable to, if they're unconscious, incapacitated through drink or drugs, or someone with mental health issues or are elderly or anything like that. It could be used if someone is unfortunately deceased, as a tool to assist in identifying an individual." The **NPCC is set to roll out OIFR more widely**, so that it's available to all forces in England and Wales sometime this year.

But what really defines the English and Welsh approach is the scale of LFR already in play. With the police and politicians highly supportive (with the caveat that Labour's approach remains unclear), it's likely we'll see much more LFR deployed in the years ahead, leaving England and Wales seemingly set to continue as – depending on your perspective – either world leaders or global outliers.

CLICK HERE
Report
Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement
ieai.mcts.tum.de

CLICK HERE
Report
A sociotechnical audit: Assessing police use of Facial recognition
How ethical and lawful is police use of facial recognition?
mctd.ac.uk

CLICK HERE
Policy
Facial Recognition Technology
The typical uses of FR technology for policing
met.police.uk

CLICK HERE
Report
Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology
files.lbr.cloud

CLICK HERE
Report
Metropolitan Police Service Live Facial Recognition Trials
An evaluation of the trials of public deployments of 'fixed plot' LFR by the MPS between August 2016 and February 2019
science.police.uk

CLICK HERE
Report
LFR deployments from 2017 to 2024
Data on South Wales Police's use of FR
south-wales.police.uk

CLICK HERE
Report
Stop Facial Recognition: The Lawless Growth of Facial Recognition in UK policing
How FR is being used and how it risks reshaping our rights
bigbrotherwatch.org.uk

CLICK HERE
Legal
R (Bridges) V Chief Constable of South Wales Police
The first case to consider the use of automated FR technology
libertyhumanrights.org.uk

CLICK HERE
Legal
Facial recognition technology needs proper regulation – Court of Appeal
R (Bridges) won his appeal against South Wales Police
adalovelaceinstitute.org

CLICK HERE
Report
MPS LFR deployments 2020 – 2022
Metropolitan Police use of LFR statistics
met.police.uk

CLICK HERE
Report
MPS LFR deployments 2023-date
Data from the Metropolitain Police on live facial recognition deployments
met.police.uk

CLICK HERE
Policy
Live facial recognition
Guidance for the overt deployment of live facial recognition (LFR) technology
college.police.uk

CLICK HERE
Legal
Live Facial Recognition: Legal Mandate
An explanation of the varied sources of law that regulate LFR
met.police.uk

CLICK HERE
Legal
South Wales Police Live Facial Recognition (LFR): Legal Mandate
An explanation of the varied sources of law that regulate LFR
south-wales.police.uk

CLICK HERE
Report
Facial Recognition Technology In Law Enforcement
Evaluation of face recognition and analysis technology
science.police.uk

CLICK HERE
Report
The Future of Biometric Technology for Policing and Law Enforcement
Exploring the future of biometric technology for UK policing
cetas.turing.ac.uk

CLICK HERE
Report
How do people feel about AI?
A nationally representative survey of public attitudes to artificial intelligence in Britain
cetas.turing.ac.uk

CLICK HERE
Policy
MPS policy – retrospective facial recognition system
Establishes policy and standard operating procedures for the use of the MPS Retrospective Facial Recognition System.
met.police.uk

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Australia and the US: early experiments in LFR

Trials of live facial recognition experienced mixed success in both jurisdictions, which seemingly encouraged a switch to retrospective use instead. However, achieving a comprehensive view of what's going on is no easy task in these forces.

Statistics & facts

2001 the first deployment of LFR in the US, at the 35th Superbowl in Tampa, Florida

5 number of positive matches from 268 targets during Queensland Police's use of FR during the 2018 Commonwealth Games

25% proportion of US law enforcement agencies estimated to have access to an FR Programme by 2016

5 key vulnerability factors in a model FR law drawn up by academics in Australia, by which police use of the technology is deemed to have an 'extreme' impact on people's rights

The Wild West the description given to the lack of regulation of FR in the US



Unlike England and Wales, which is openly rolling out live facial recognition (LFR), it's much more difficult to map current police practice in Australia and the US. While both jurisdictions have trialled LFR in the past (with mixed success) before seemingly switching to retrospective facial recognition (RFR), experts told Policing Insight that understanding what's really going on in these two countries is no easy task.

In April 2018, the city of Gold Coast, Queensland played host to the 21st Commonwealth Games. Prior to the Games, the Australian Federal Police **installed FR capabilities** on cameras within the city's public transport network. In response, Queensland's then Privacy Commissioner, Philip Green, **raised concerns** about the potential for a "false-positive problem" and called for a "proper privacy impact analysis". The police's purported rationale for LFR was that it could help identify terror suspects attempting to access sporting venues.

Ultimately, the technology didn't have the desired effect. In May 2019, **ABC News shared details** from Queensland Police's evaluation report of this LFR deployment. It was only released on the order of the Information Commissioner, after the police made attempts to block its publication.

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition around the world

ABC News reported that the police found none of their 16 most important targets. The system used a database of eight million images (a further 38 million images were planned for inclusion, but weren't able to be used). The police also expanded the FR system's focus mid-way through the event, targeting other potential criminals rather than just suspected terrorists. Even with this broader scope, it still found only five of the 268 police targets.

Further developments

There's no obvious evidence of other LFR use by the police in Australia. However, between 2019-2020, numerous forces did trial Clearview AI – a company which offered a tool allowing officers to compare images to a database of faces scraped from social media sites. The Australian Information and Privacy Commissioner later **ordered the company to cease** collecting data in this way. It also **instructed the Australian Federal Police** to tighten their privacy practices.

In 2021, Australia's Human Rights Commission responded to this (and other FR developments) with **an extensive report on new technologies**. It recommended "a moratorium on the use of biometric technologies, including facial recognition, in high-risk areas", until new legislation was in place. It stated: "All Australian governments should work co-operatively to introduce legislation that regulates the use of facial recognition and other biometric technologies."

The Australian Government did not accept this finding. In New South Wales, **the police reportedly suggested that FR use was "misunderstood"** and did not commit to any pause. A **December 2023 law** has, however, reduced the circumstances in which police can use some RFR tools.

Current use

An independent 2021 review of FR tech for New Zealand Police made a revealing comment. It said: "Police forces across Australia's states and territories are reported to use FRT, but it is difficult to obtain information and statistics on use." There is notably much less transparency in Australia than in England and Wales.

In an interview with Policing Insight, Lauren Perry, a Policy Specialist at the Human Technology Institute (based at the University of Technology Sydney) said the same: "FR is being used by police at federal and state levels, with several unverified uses of the technology reported by the media, alongside a few formalised use cases confirmed by police themselves. There appears to be a lot of 'trialling' of the technology. But everyday people are really not that aware of what's going on."

She also suggested that, at this stage, there is limited evidence of police considering live uses of FR: "Most of the case studies I've seen focus on retrospective uses of FR."

In 2022, Ms Perry and two co-authors (Professors Nicholas Davis and Edward Santow), produced their own '**model law' for uses of FR** in Australia which seeks to address significant gaps in legal guardrails around applications of FR technologies. "Our model law applies a risk-based approach to regulating different uses of FR, to enable the responsible use of the technology while mitigating harms," explained Ms Perry.

> **"There appears to be a lot of 'trialling' of the technology. But everyday people are really not that aware of what's going on."**
>
> **Lauren Perry, Human Technology Institute, University of Technology, Sydney**

"We recognise that FR tools and technologies may be useful to police in certain circumstances, however, there are significant risks to people's human rights which need to be balanced and protected. Our Model Law contains a special regime for the use of FR in the law enforcement and national security context, including requirements around technology performance, data standards, human review and accountability mechanisms."

Returning to LFR, it's true that it hasn't been confined to that 2018 Commonwealth Games alone. In the world of Australian sports, it seems increasingly common. **An investigation by consumer advocacy group CHOICE** found that Sydney and Melbourne Cricket Grounds, the Qudos Bank Arena, and Sydney's Allianz Arena all use it. Adelaide United FC's Coopers Stadium and AAMI Park are **confirmed as doing the same** too.

The 'Wild West'

Given the strength of its technological offering, it's little surprise that the USA saw one of the very first uses of LFR. It took place over 20 years ago at one of the largest sporting events in the world: the Super Bowl.

The 35th iteration of this event – contested by the Baltimore Ravens and the New York Giants in January 2001 – was held at the Raymond James Stadium in Tampa, Florida. At the turnstiles, the 70,000 people in attendance each had their faces scanned against a watchlist of criminals.

It was a remarkably early deployment of LFR, a full 17 years before the Gold Coast Commonwealth Games, and reflects what experts told Policing Insight is the defining feature of the US approach: a 'Wild West' model in which FR regulation remains extremely limited.

Ira Reese, CTO of Global Security Innovative Strategies and a Member of the National Academies of Sciences, Engineering and Medicine's Committee on FR, explained: "What's missing in FR is what's not missing around DNA and fingerprints. At this point in time, FR in the United States is more or less equivalent to the Wild West."

Chief Philip Lukens, an AI and policing expert from the International Association of Chiefs of Police and a Law

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition around the world

Enforcement Advancing Data and Science (LEADS) Scholar at the National Institute of Justice, made a similar comparison: "[FR today] is kind of like when the dot-com craze hit in the 90s. Everybody was all over it for five years and then over time, it began to take shape. But it was the Wild West for a good five years."

The lack of standards is matched by an absence of transparency, according to Clare Garvie, a lawyer with the Fourth Amendment Center and expert on police FR. "One of the biggest challenges with understanding how widespread it is in the US is the complete lack of transparency. Agencies aren't forthcoming about which systems they purchase and how and when they implement them. The systems we find out about are largely due to public records requests and journalists or advocates asking for information, rather than agencies volunteering it."

> **"What's missing in FR is what's not missing around DNA and fingerprints. At this point in time, FR in the United States is more or less equivalent to the Wild West."**
>
> **Ira Reese, CTO, Global Security Innovative Strategies**

US law enforcement

Ms Garvie explained how police use of FR has developed in the US. "FR was first adopted in around 2001. The earliest known adopters were a county sheriff's department in Florida and the Michigan State Police. Then there were a couple of pilot projects in the early 2000s with mobile FR devices taken from the wars in Afghanistan. They didn't really go anywhere and the consensus was that they weren't very effective.

"In 2012, there was a much more rapid adoption as improvements in, and availability of, the technology increased. In 2016, we saw that speed up again… And we estimated then that at least a quarter of all law enforcement agencies had access to an FR programme, either their own or through some sort of informal or formal partnership with another agency."

There has been previous exploration of LFR too, she continued. "One trend is lots of interest in the use of FR as a surveillance tool: connecting FR to live video cameras for situational awareness and to identify people in real-time. My research found a handful of agencies ordered projects like that between 2014 or so and 2019, including Chicago, Detroit, New York City and the Secret Service here in Washington DC.

"There was widespread and pretty immediate backlash to that type of system. So, as far as I know, all those systems have been shut down. Even while FR has been widely adopted, use in real-time – in its surveillance capacity – has, to my knowledge, largely disappeared." It's also true that some jurisdictions, such as San Francisco, have gone further and **banned FR altogether**.

Chief Lukens, who most recently served as Chief of Police in Alliance, Nebraska, offered roughly the same assessment of the current situation, describing the use of LFR as "very, very rare at this point in time". "I only know of a handful of agencies that are even trying live, and I think those are very much in the fledgling stages of tests. Pretty much anybody that's utilising it is using RFR," he added.

This aligns with what some police forces say publicly. For example, the New York City Police Department admits to using RFR – indeed, it courted controversy when it used RFR to **track down a Black Lives Matter activist in 2020** – but its **guidance states** that LFR isn't used. Similarly, Mr Reese noted that the 2024 **report from the National Academies of Sciences, Engineering and Medicine's Committee on FR** "did not pick out" LFR use by US law enforcement.

The USA and Australia have been on similar journeys around FR. From some early (and much-criticised) use of LFR by law enforcement, the switch has been towards retrospective instead. But it is tough to know this for sure, especially in the USA, where the 'Wild West' means there's little regulation and, Ms Garvie suggests, little transparency either.

CLICK HERE
Legal
Commissioner initiated investigation into Clearview AI, Inc.
Information and Privacy Commissioner ordered the company to cease collecting data from social media sites
austlii.edu.au

CLICK HERE
Policy
AFP ordered to strengthen privacy governance
Australian Federal Police (AFP) failed to comply with its privacy obligations in using the Clearview AI facial recognition tool
oaic.gov.au

CLICK HERE
Report
Final Report: Human Rights and Technology
A roadmap for Australia to seize the opportunities and address the threats from new technologies
humanrights.gov.au

CLICK HERE
Legal
Identity verification bill passes with 38 changes
Senate squeezed in privacy enhancements.
ia.acs.org.au

CLICK HERE
Report
Facial Recognition Technology: Considerations For Use In Policing
Use of FR technology in policing in New Zealand.
police.govt.nz

CLICK HERE
Report
Facial recognition: Towards a model law
Report calling for Australia to establish a dedicated facial recognition law
uts.edu.au

CLICK HERE
Policy
NYPD Questions and Answers: Facial Recognition
New York Police Department policy on FR
nyc.gov

CLICK HERE
Report
Facial Recognition Technology
Current Capabilities, Future Prospects, and Governance
nap.nationalacademies.org

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

The Dutch model: a unified national approach

What really makes the Dutch Police stand out is their highly transparent and well-structured approach to FR, accompanied by the regular publication of data, a new ethical framework, and efforts to engage internationally.



> **"We saw that the technology was ready to work on the big national databases we have of faces from suspects and convicts. We thought that if we could do searches with faces, like we run searches of fingerprints, that could offer interesting benefits on a national level."**
>
> **Chief Inspector John Riemen, Lead Specialist on Biometrics, Dutch Police**

When it comes to police use of facial recognition (FR), the Dutch model offers an interesting case study. In contrast to England and Wales, there's no suggestion that law enforcement is exploring the potential for live facial recognition (LFR). At the same time, they're much more advanced than some other countries, who are just beginning to explore wider adoption of retrospective facial recognition (RFR).

But what really makes the Netherlands stand out is the highly transparent and well-structured approach they've taken to FR, accompanied by the regular **publication of data**, a new **ethical framework**, and **efforts to engage internationally**. Policing Insight spoke to Chief Inspector John Riemen, the Dutch Police's Lead Specialist on Biometrics, to understand more.

From first trials to fully-fledged tools

Ch Insp Riemen has played a key part in the Dutch National Police's journey around FR, having been manager of the Netherlands National Criminal Automated Biometric Identification System (ABIS) since February 2004.

He explained: "We started the pilot in 2014, when we saw that the technology was ready to work on the big national databases we have of faces from suspects and convicts. We thought that if we could do searches with faces, like we run searches of fingerprints, that could offer interesting benefits on a national level. And it was quite a successful pilot. We discovered that we could find people in our database by comparing two faces using facial recognition, with expert human input to verify the result."

After a serious incident in 2014, senior officers were increasingly focused on improving their ability to identify suspects – something that helped spur the development of FR. "It convinced the Deputy Chief of Police that this tool would help. He thought: 'I have an enormous database of faces, but if I don't have the right tools to search it, having all this data is irrelevant.' He assigned me the job of deploying – as fast as possible – an FR tool and process that was robust enough to do those searches.

"By the end of 2015, we were able to search faces based on images we got from investigation teams. We can compare that image to our police database and, if we get an order from a public prosecutor

Continued overleaf ↘

Statistics & facts

2014	launch of the first Dutch Police's pilot of FR
No-go	the Dutch Police approach to LFR in the wake of the limitations of the EU AI Act, with the service focusing instead on RFR
3	the number of humans in the loop to confirm a positive face match, compared to just one algorithm
218k	the number of unpermitted photos of innocent people removed from Dutch Police databases in 2021
Football	some Dutch politicians have called for a less restrictive use of FR in the private sector, including to tackle violence at football matches

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight



and support from an investigative judge, to a special database of migrants too."

By 2016, the face-comparison programme was up and running. Crucially, this is an example of RFR, rather than any live application – something that holds to this day. "We're interested in what the UK is doing with LFR, especially in the Metropolitan Police, but that's a no-go for us because of the limitations emerging in the **EU AI Act**. We're fully focused on post-event evaluations in the Dutch Police."

Despite these comments, it's not clear that the EU AI Act would prevent European police forces from using LFR – in fact, it might even enable it. We'll explore that in the next part of this report, when we turn to the potential growth of **FR in Sweden and Ireland**.

Humans in the loop

Human experts are at the heart of the Dutch model. The process – **set out in a diagram from the World Economic Forum** – begins with an investigating officer asking for an image to be compared to existing databases. To do this, the Dutch Centre for Biometrics uses its 'CATCH system' which employs an FR algorithm from IDEMIA. This produces a list of potential matches who might be the person in the original picture.

At this stage, a human facial examination expert examines the list. If they spot a match, the original image and the suspected match are sent on to two more human experts. If these two experts also agree, the match is shared back with the investigation team. The robot is outnumbered here: there's three humans in the loop every time and just one algorithm.

There are some limitations to this approach, however. Ch Insp Riemen told us the force had been using an algorithm purchased in 2015, but then "we recently changed the algorithm and saw a spectacular increase in hits".

The data to prove that isn't yet available, but the limitations of the old system are clear from the **police's own data**. Out of 1,098 images put forward for analysis in 2022, 631 were suitable for CATCH and only 130 led to a match. In 2021, 913 images were suitable for analysis – but these yielded only 104 matches in total. It's possible, of course, that this is because those individuals weren't in the database; but it's also possible that a more effective algorithm might get more hits, as Ch Insp Reimen hopes.

Two other problems are worth mentioning. First, the Dutch Police were previously found to have photos in their databases which should have been deleted, including those of innocent people or those who are no longer suspects. In 2021, **it was reported** that they'd removed 218,000 of these unpermitted photos in just a single year.

The second is that CATCH remains poorly understood by some in Dutch policing, Ch Insp Riemen claimed. "A lot of colleagues still don't know we have this technology in-house. We're only reaching a small number of colleagues, it's often a word-of-mouth thing. If people don't search on our website for FR, they'll sometimes never find out that we exist!"

Private use

As in many other countries, the Netherlands has had FRT developments in the private sector too, and again some of these extend beyond what the police are prepared to do. One notable example involved a Dutch supermarket, which used LFR cameras to tackle shoplifting. According to the **Dutch Data Protection Authority**: "The technology scanned the face of everyone who entered the store and compared it to a database of people who had been banned from entering stores. The faces of people who had not been banned were deleted after several seconds."

After media reports that this technology was being used, the Authority got involved. Two days later, on 8 December 2019, the supermarket disabled the tech – but told the regulator that it wanted to start using it again in future.

In January 2021, the Authority gave its verdict. It issued a formal warning to the company and said that it had not shown that LFR was necessary for security or authentication purposes. The regulator's Deputy Chair, **Monique Verdier put it simply**: "The only example that the law gives is for the security of a nuclear power plant. The bar is therefore very high. Preventing shoplifting is of a completely different magnitude than preventing a nuclear disaster."

However, some **politicians have reportedly argued for a less restrictive approach** to private sector use of FRT in the context of football matches. In June 2023, one Dutch parliamentarian said: "You see that all kinds of unsafe things happen in the stadiums: brawls, insults, and racism. And then facial recognition is not allowed. That doesn't make things safer." Other politicians made similar comments at the time. But, from the police perspective, the approach is much simpler, at least for now; it's RFR and RFR alone in the Netherlands.

CLICK HERE
Report
Centrale Automatische TeChnologie voor Herkenning (CATCH)
Police data on FR usage
politie.nl

CLICK HERE
Report
A Policy Framework for Responsible Limits on Facial Recognition
Use Case: Law Enforcement Investigations
weforum.org

CLICK HERE
Legal
AI Act
The EU's 27 member states have unanimously endorsed the AI Act
artificialintelligenceact.eu

CLICK HERE
Article
Police remove 218,000 photos from facial recognition database
Dutch police clear up FR database
dutchnews.nl

CLICK HERE
Article
Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology
Supermarket wanted to switch its FR system back on
edpb.europa.eu

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

New Zealand and Canada: little chance of 'live'

In response to several controversies, both jurisdictions have developed clearer guidance around facial recognition technology that appears to only permit police use retrospectively.

Though New Zealand and Canada each have their own distinct stories around the police use of facial recognition (FR), there are interesting similarities. Both had a controversy around the use of Clearview AI; both have gradually developed clearer guidance around the use of FR; and both, for now, appear set to focus on retrospective facial recognition (RFR) alone.

New Zealand's FR journey

To understand how FR has developed in New Zealand, Policing Insight spoke to two leading experts: Dr Nessa Lynch, Matheson Lecturer in Law, Innovation & Technology, University College Cork, and Dr Andrew Chen, Senior Research Fellow at Koi Tū (the Centre for Informed Futures) at the University of Auckland. They co-authored an an influential 2021 report which shapes New Zealand Police's FR policy to this day.

> **"Police will not deploy any Live FRT and will engage in wider public consultation before any possible change to this position is made."**
>
> **New Zealand Police official statement**

Both academics pointed to Clearview AI – a company which had a tool that allowed officers to compare images to an online database of faces scraped from social media sites – as the first major part in New Zealand's story. In this case, **police officers used the tool without approval** from senior leaders or ministers.

Dr Lynch suggested that this 2020 incident did cut through: it was "reported on quite heavily by journalists" and "bubbled up into the public consciousness". However, Dr Chen said that it was a small use of FR in reality: "New Zealand got off lightly on Clearview because we basically got a free trial, put in some faces, it didn't work well, and so the trial ended… The use of it never got far enough to warrant privacy commission fines or bans, like in Australia and Canada."

In the same year, New Zealand's state agencies – including the police – adopted a government-wide **Algorithm Charter**. This set out how the state would approach the future use of AI. "It does two things," explained Dr Chen. "It introduces a risk calculation that's categorical rather than quantitative, essentially a 'likelihood times impact' calculation to decide whether or not the charter should apply in that case. And then there's a set of principles like transparency, human rights, and ethics, giving people an ability to challenge decisions. The usual things that are now commonly accepted as being good when using data and technology."

In 2021, the police also adopted a **New Technology Framework** that operates on similar lines, but adapted to a law enforcement context. It sets out 10 principles that policing should follow when adopting new tools, covering things such as necessity, lawfulness, privacy, and transparency.

RFR and LFR

In November 2021, Dr Chen and Dr Lynch published their **independent report on the use of police FR in New Zealand**.

It found that policing's "current or imminent planned use of facial recognition technology (FRT) is limited and relatively low risk", with no evidence of any live facial recognition (LFR) being deployed. And it called on NZ Police to "formally pause any consideration of deployment of live automated FRT… for a minimum time period and make a public statement or policy to that effect". This 'pause' should only end, they added, if a number of significant conditions are formally met.

The police ultimately accepted all 10 recommendations in the independent report. In its **formal response**, NZ Police made a crucial commitment: "Police will not deploy any Live FRT and will engage in wider public consultation before any possible change to this position is made." This pause is still the policy today.

Continued overleaf ↘

Statistics & facts

10	principles contained in the New Technology Framework adopted by NZ Police in 2021
Pause	the position of NZ Police in relation to LFR, which will not change without "wider public consultation"
25	the number of Foodstuff's North Island supermarkets currently using LFR on a six-month trial, which has prompted an inquiry by the NZ Privacy Commissioner
14	the number of Canadian privacy commissioners jointly calling for calling for a new legal framework setting "appropriate limits" on the police use of FR
17	key considerations for policing documented in guidance on the use of FR published by the Information and Privacy Commissioner of Ontario

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition around the world



Though Dr Chen spoke to us in his academic capacity, he also serves as NZ Police's Chief Advisor for Technology Assurance, giving him a unique insight into how FR is actually used. He explained that RFR is now regularly employed: "Before 2020, there was very limited use and in very niche applications. One example was in relation to child sexual abuse imagery. Since 2020, everything NZ Police has done has been in retrospective offline usage. There's no live usage, in contrast to other jurisdictions.

"We have a couple of teams who use FRT to scan footage for things that have happened, rather than sitting there manually watching hours of footage… For example, if there's been a murder and neighbours have provided CCTV footage for review. There's also a facial matching capability slowly being developed, so if we're given an image of somebody, we can check our database to see if it's somebody we know." As with the Netherlands, this is run through the biometrics office. It's a "tightly controlled capability, where people make requests to this small team of three to four people who operate the software, make an assessment, and return the result," added Dr Chen.

Though **comments by Deputy Police Commissioner Tania Kura** caused a stir – she said that New Zealand needs an "open discussion" about FR use in retail spaces – both Dr Lynch and Dr Chen agree that LFR isn't likely to be used by NZ Police anytime soon.

Dr Lynch said: "As the police have stated publicly, they don't use that tech and it's not under active consideration. I think there's a chance to learn some lessons, particularly from police forces in the UK, about what's gone wrong." Dr Chen agreed. "There's just no 'social licence' for that in New Zealand; it's highly, highly controversial… I think there would be very little acceptance of police doing it in a live setting, in the way that maybe it's been done in the UK. Another barrier is that New Zealand Police actually own very few cameras."

> **"There's just no 'social licence' for that in New Zealand; it's highly, highly controversial… I think there would be very little acceptance of police doing it in a live setting, in the way that maybe it's been done in the UK."**
>
> **Dr Andrew Chen, Senior Research Fellow, University of Auckland**

Once again, it seems that the private sector is making the first move around LFR. In April 2024, New Zealand supermarket chain Foodstuffs began a six-month trial of LFR in 25 North Island stores, aiming to reduce retail crime. New Zealand's Privacy Commissioner Michael Webster is **running a parallel inquiry** into this new and controversial development.

Canada's approach

As in New Zealand, one of Canadian law enforcement's first brushes with FR involved Clearview, as Patricia Kosseim, Information and Privacy Commissioner of Ontario, told Policing Insight: "We know that, at one point, police services in Canada were making use of third-party services offered by Clearview AI. That really hit the news and brought this debate into public consciousness."

After those **2020 media reports** revealed that various Canadian police forces were trying out Clearview, the Office of the Privacy Commissioner of Canada launched a joint investigation with its regional counterparts in Quebec, Alberta and British Columbia. In response, the company decided to stop offering FR in Canada in July 2020. The **final investigation report**, published in December 2021, ordered Clearview to avoid doing business in those areas and delete the information they'd already collected.

This led to a flurry of additional activity. In May 2022, 14 Canadian privacy commissioners – from the federal, provincial and territorial levels – **issued a statement** "calling for a new legal framework that

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition around the world

sets out appropriate limits on police use of FR". They also produced some interim guidance, suggesting that any police use of FR should have clear authorisation, privacy protections and independent oversight. It should also follow necessity and proportionality rules.

Shortly afterwards, a **Canadian parliamentary inquiry on FRT published its own report**. Testimony from the Royal Canadian Mounted Police (RCMP) revealed that the force used FR to "identify victims of sexual exploitation, human trafficking and missing persons". And Toronto Police acknowledged use of RFR to compare suspect photos to a mugshot database.

In total the Committee produced 19 recommendations. It argued that Canada's Government should: "Impose a federal moratorium on the use of FR technology by (Federal) policing services and Canadian industries unless implemented in confirmed consultation with the Office of the Privacy Commissioner or through judicial authorization." **The Government response** "acknowledge[d]" this recommendation, but did not commit to it in full.

> **"We know that many police services in Canada may have FR features they can turn on in body-worn cameras. We don't have evidence that they're being used in this way, but we've asked police in Ontario to hold off on using that, until they've done a full risk assessment and consulted our office."**
>
> **Patricia Kosseim, Information and Privacy Commissioner of Ontario**

Ontario – leading the way

Ms Kosseim told Policing Insight about two main examples of FR she was aware of. "As well as past use of Clearview AI, we know that many police services in Canada – depending on the vendors they use – may have FR features they can turn on in body-worn cameras. We don't have evidence that they're being used in this way, but we've asked police in Ontario to hold off on using that, until they've done a full risk assessment and consulted our office. And the other use case is these police-held mugshot databases, which contain images that they are authorised to collect and use to identify suspects."

She continued: "The police in Ontario told us: 'These national guidelines are all well and good, but we need something more granular and specific to us.' So we've developed this specific guidance on FRT use with mugshot databases which, though there are still many risks associated with it, are probably at the lower end of the risk spectrum."

Published in January 2024, **the guidance** is pretty comprehensive. It sets out 17 key considerations for policing, covering pre-implementation, operational issues, and programme review and evaluation. The Commissioner pointed to key risks it addresses, including the reality that "mugshot databases may reflect a history of disproportionate police practices", the failure to delete some images as legally required, and the need for community consultation, pilot programmes, training and high-quality images where possible. Many of these concerns are explored later in this report.

While there's no national commitment from Canadian policing to rule out LFR (in contrast to New Zealand), it seems that both countries are in roughly the same place.

From their early Clearview controversies, each has gradually seen more scrutiny and guidance around police use of RFR. Even the retail sector's story has parallels in the two countries, with a **controversy in Canada** after four Canadian Tire stores in British Columbia were found to have used LFR. From the policing side, however, that doesn't look likely; for now, there's little chance of live.

CLICK HERE
Article
Australian privacy office orders Clearview AI to delete harvested images – what could it mean for NZ?
Clearview AI ordered to cease collecting images of Australians
bellgully.com

CLICK HERE
Policy
Algorithm charter for Aotearoa New Zealand
An initiative for the government's data system
data.govt.nz

CLICK HERE
Policy
New Technology Framework
A framework to assist decision-making on new technology
police.govt.nz

CLICK HERE
Report
Facial Recognition Technology: Considerations For Use In Policing
Use of FR technology in policing in New Zealand.
police.govt.nz

CLICK HERE
Policy
Police release findings from independent expert review of Facial Recognition Technology
Review provides police with detailed advice on FR
police.govt.nz

CLICK HERE
Policy
Recommended legal framework for police agencies' use of facial recognition
Calls for a new legal framework that limits police use of FR
priv.gc.ca

CLICK HERE
Report
Facial Recognition Technology And The Growing Power Of Artificial Intelligence
Report on Access to Information, Privacy and Ethics
ourcommons.ca

CLICK HERE
Report
Summary of recommendations from the Facial Recognition Technology report
Letter summarising findings of the above report
ourcommons.ca

CLICK HERE
Policy
Facial Recognition and Mugshot Databases: Guidance for Police in Ontario
Office of the Information and Privacy Commissioner of Ontario
ipc.on.ca

CLICK HERE
Report
Canadian Tire Associate Dealers' use of facial recognition technology
The OIPC investigation into the use of FR technology
oipc.bc.ca

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Ireland, Sweden and the EU AI Act

Ireland and Sweden offer a revealing joint case study where governments have taken steps which could make law enforcement use of facial recognition much more common.

As our final deep-dive in this section, Ireland and Sweden offer a revealing joint case study. In both countries, governments have taken steps which could make law enforcement use of facial recognition (FR) much more common. At the same time, the precise approach to different types of FR varies. Ireland is much more conservative than Sweden, with the former explicitly ruling out live facial recognition (LFR). And the **EU AI Act** is set to play a major role too, with its relevant regulations due to come into force at the end of 2024.

Ireland's 'general scheme' for FR

An Garda Síochána (the Republic of Ireland's police force) has used retrospective facial recognition (RFR) for some time, its Chief Information Officer Andrew O'Sullivan told Policing Insight. "Since 2017, we've had a product – it's listed in our public record – which uses FR. It's in use by the Garda National Cyber Crime Bureau whose responsibilities include investigation of child sexual abuse material."

> **"Even in relatively small investigations, we could have thousands or tens of thousands of hours of footage. Anything we can do to narrow that down and present it like we do for [child sexual abuse material] investigators is where we'll look first."**
>
> **Andrew O'Sullivan, CIO, An Garda Síochána**

But the Irish Government wants the Garda to go further. In 2022, the Minister for Justice tried to amend a bill moving through the Oireachtas (the Irish Parliament) to let the Garda use FR more widely. These proposals were eventually dropped after civil society resistance, including a **highly critical letter** signed by seven universities and 13 NGOs that was sent to *The Irish Times*.

A year later, the Government tried again, publishing the **Draft General Scheme Of Garda Síochána (Recording Devices) (Amendment) Bill** to permit FR use by police. **The Government said** it would enable "retrospective searching of images which are legally in the possession" of police under three conditions: if a serious offence is suspected, it's necessary and proportionate, and a chief superintendent gives authorisation.

In a **submission to the Joint Committee on Justice**, the Garda set out nine intended FR use cases, though many of these are really about tracking objects rather than faces. For example, the Garda refer to "object clustering – having identified an object of interest, the ability to search for all occurrences of it". But it also covers searches for images "in a digital evidence series for occurrences of a specific person of interest's image" and of "database[s] of facial images (with associated identity) for a match with an image". In other words, RFR.

Mr O'Sullivan pointed to the huge amount of digital evidence available now, stating: "Even though a trained facial examiner can go through thousands of images a day, it becomes very impractical very quickly to go through that kind of volume… Even in relatively small investigations, we could have thousands or tens of thousands of hours of footage. Anything we can do to narrow that down and present it like we do for [child sexual abuse material] investigators is where we'll look first."

He noted that the use of LFR isn't on the cards at all. In fact, he claimed, the Garda "requested it to be excluded": "We have no interest in doing this because it runs counter to our philosophy."

As part of its scrutiny work, the Irish Joint Committee on Justice brought together representatives of the police, government and those critical of FR for a public hearing in mid-February. Policing Insight interviewed four of those who took part (including Mr O'Sullivan).

Dr Elizabeth Farries, Co-Director of the UCD Centre for Digital Policy, offered a highly sceptical view: "Using that level of detailed surveillance of our biometric data, those most immutable and sensitive parts of us, to catch specific individuals is highly problematic." She added that the Garda's stated use cases "have changed over time – there's just no consistency there".

Continued overleaf ↘

Statistics & facts

3	the conditions in a draft bill on police use of FR put forward by the Government in 2023
9	the number of FR use cases put forward by the Garda to the Joint Committee of Justice which is considering the bill
Excluded	the request from the Garda in relation to the police use of LFR, with the service having "no interest" in using the live technology
2,500	the number of police surveillance cameras in Sweden (increased from 1,600) as a part of police measures to tackle gang-related crime
3	conditions under which European police forces will be able to use LFR under the new EU AI Act, with the authority of a judge

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition around the world

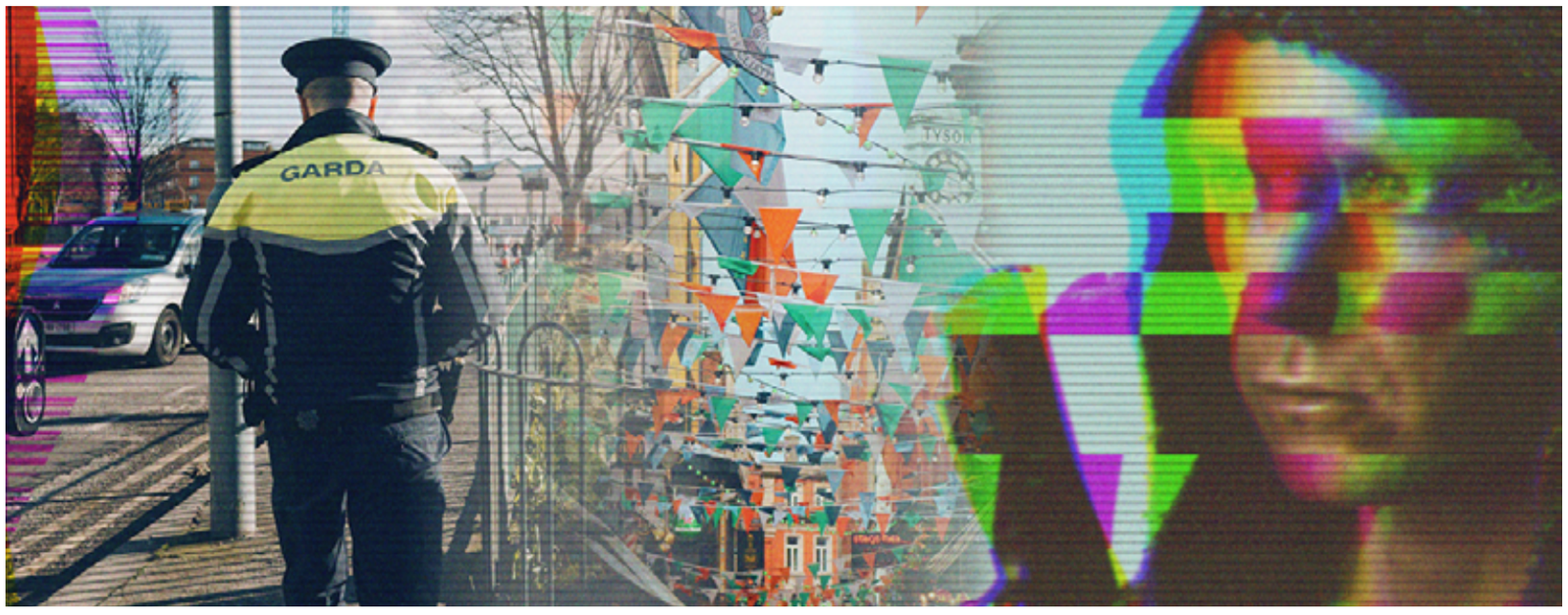
Dr Nessa Lynch, Matheson Lecturer in Law, Innovation & Technology, University College Cork, suggested that there just isn't enough clarity in the current proposals. "In Ireland (unlike New Zealand and other jurisdictions), you only get the 'heads of the bill' at the pre-legislative scrutiny stage, which are quite general. I think almost all the expert witnesses were coalescing around the point that you really need to know the exact use case before you can judge proportionality." That's because there are some RFR uses which she feels are "justified", while others are more contentious.

By far the most contentious is the final use case presented by the Garda: searching a database of facial images for a match. Mr O'Sullivan downplayed the likelihood of this, telling Policing Insight: "We currently don't have such a database – a national computer with images that we can search against. We don't have the capabilities to do that, and it's a much lower priority for us than use cases one to eight." In fact, he continued: "We may never build our own database… [and] have no immediate plans to either." He suggested that the inclusion of this use case was partly to ensure Ireland can fully exploit the Schengen biometric database in future, which is set to include some FR capabilities.

But David Murphy, Assistant Commissioner of the Irish Data Protection Commission, agreed that more clarity is preferable. "As far as we're aware, we haven't seen any proposals for building up an FR database. Our understanding is that it's investigation-specific and limited use cases, but again we'd want to see that either in the Bill or in the future Code of Practice."

Eventually, the Justice Committee offered the same opinion. In its **final report**, it called for "redrafting" to make clear whether the police are planning to compare images to a database and, if so, which databases they'll use. It also recommended monitoring how any FR is actually deployed, and testing to reduce disproportionality risks, among various other measures.

It seems that the draft bill is likely to pass, though its exact shape may only become clear in the coming months. At the very least, LFR won't be on the table. The real question is what kind of RFR we're likely to see being used by the Garda.



> **"As far as we're aware, we haven't seen any proposals for building up an FR database. Our understanding is that it's investigation-specific and limited use cases."**
>
> **David Murphy, Assistant Commissioner, Irish Data Protection Commission**

Sweden: using FR to fight gang crime

In Sweden, the Government has recently made similar moves to those in Ireland, with plans that are likely to see a growing use of FR by the police. Some very limited FR has already been applied by Swedish law enforcement, according to Marie Eneman, Associate Professor in Informatics at the University of Gothenburg: "The police in Sweden are allowed to use RFR already, but not LFR."

There was also a Clearview AI scandal several years ago, where "a number of police officers downloaded the application to their mobile phones to identify victims and offenders… after they had been recommended this during a training course at Europol". The **Swedish Authority for Privacy Protection wasn't impressed**, and fined the Police Authority 2.5 million Swedish krona in 2021 (around £217,000 at the time.)

Sweden's debate about public safety is consumed by the growing threat of gang warfare, with violent crime increasing burdens on the police in a country which has historically been very peaceful. To tackle this, the Swedish Government has been bolstering police powers. Last year, they gave them the legal right to conduct surveillance to tackle gang-related crime, something that was only available to the intelligence service (Säpo) before this. Then in October 2023, **Justice**

Continued overleaf

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

> **"The political will and ambition is to increase the number of cameras and [explore] the possibility of using LFR... The political pressure is strong to make it even easier for law enforcement to use powerful surveillance technology, such as LFR, in the near future."**
>
> **Marie Eneman, Associate Professor of Informatics University of Gothenburg**

Minister Gunnar Strömmer announced a new "rapid inquiry". This would last six months and present new ideas for enhancing police capabilities, including the use of FR cameras. There are **related plans to boost the number of surveillance cameras** held by the police from 1,600 to 2,500 in 2024.

Prof Eneman told Policing Insight: "The political will and ambition is to increase the number of cameras and [explore] the possibility of using LFR. We now have a right-wing government that co-operates with the Sweden Democrats. The political pressure is strong to make it even easier for law enforcement to use powerful surveillance technology, such as LFR, in the near future."

The EU AI Act might even help with that, Prof Eneman explained: "When the AI Act is introduced as law, the Swedish police will be able to use AI both on already collected material from cameras, and also in real-time [under various conditions.]"

On 3 June, these predictions appeared to have been proven right. It was **reported** that Kazimir Aberg, the lawyer who headed up the rapid inquiry, told the press: "Facial recognition in real-time in public places should be allowed for crime-fighting purposes to the extent that the EU's AI regulation allows."

While details are understandably limited at this stage, there is some extra information. Mr Aberg said LFR should only be used with judicial authority (as required under the EU AI Act), for crimes which carry at least four years in prison, and for specific investigations. The Government now appears set to start using LFR on a **database of 40,000 images**, though exactly when this will happen isn't yet clear.

The EU AI Act – the impact of a partial ban on LFR

Though many countries covered in this report won't be affected by the EU AI Act, this new legislation is set to transform the European approach to FR. For Ireland, Sweden, the Netherlands and other EU member states, its implications could be extremely significant.

Ella Jakubowska, the Head of Policy at the European Digital Rights (EDRi) Network, has followed this law closely. She confirmed that after the final passage of the **full text of the Act** (which is currently planned for the 21 July - though may still change) the specific rules on police FR only fully come into force six months later. But RFR is unlikely to be affected, she argued: "The text claims to put in a couple of safeguards around retrospective use. But as far as we're concerned, those limitations are lip service. They're not going to do anything meaningful." And crucially, it's only a partial ban on LFR too.

European police forces can use LFR, with a judge's authority, in cases "limited to certain specific missing persons, certain specific crimes and a specific imminent threat of a terror attack". To make use of those three conditions, "member states first need [to pass] a national authorising law" setting out safeguards and their intention to use FR. In other words, the Act creates a new hurdle: until countries pass a national law of their own, any police LFR is, by default, illegal.

Constrainer or enabler?

The full implications of the Act are difficult to understand at this stage. A complete ban would obviously offer certainty. But, while the new Act sets some constraints – LFR can only be used in response to some specific threats (even if the list is fairly broad) – it also opens the door to LFR that meets these conditions, something the Swedish example might already provide evidence for.

As Ms Jakubowska put it: "We've been really worried about the normalising or legitimising effect of an EU law that says there are some cases where FR can be deployed. We've long said FR is a fundamental violation of people's rights and shouldn't be allowed in any format. And if it's allowed in the EU, there can also be a knock-on effect across the rest of the world."

For supporters of FR in policing, this compromise might be attractive. It includes safeguards and appropriate limits, allowing the police to use LFR in cases where it's operationally valuable. They can use it to frame out a new national law, letting the police use LFR for the very first time. For opponents, it means the battleground shifts down from the supranational to the national. For Ms Jakubowska and EDRi, the "next step is mobilising, as many states would have to introduce national implementing laws [to use LFR.] We need to make sure that they can't do that."

Perhaps then, the EU AI Act is really just the end of the beginning. The real battle over police use of LFR across Europe starts now.

CLICK HERE
Legal
Artificial intelligence (AI) act
Legal framework for AI development and use within the EU
consilium.europa.eu

CLICK HERE
Article
Garda use of facial recognition technologies unnecessary and disproportionate
It may have significant chilling effects
irishtimes.com

CLICK HERE
Legal
Draft General Scheme Of Garda Síochána (Recording Devices) (Amendment) Bill
gov.ie

CLICK HERE
Article
Minister McEntee receives Cabinet approval for draft Facial Recognition Technology Bill
gov.ie

CLICK HERE
Report
Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023
data.oireachtas.ie

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Approaches to FR around the world

It's impossible to cover every global development in facial recognition, but there are many important cases that have affected the global debate. From authoritarian states to much closer to home, here's a flavour of what else is going on around the world.

Scotland

Despite its geographical proximity, Scotland has taken a very different approach to facial recognition (FR) when compared with England and Wales. Though Police Scotland included a brief reference to live facial recognition (LFR) in its **10-year strategy** (which expires in 2026), this has led to no actual deployments. A 2020 **Scottish Parliament report** argued there would be "no justifiable basis" for police investment in LFR. And the Scottish Biometrics Commissioner **noted** earlier this year that: "Police Scotland has never deployed LFR." No trials have been conducted as yet either. Any attempts to use LFR might attract greater political criticism than in England and Wales, especially given the current government's highly progressive political outlook. However, like other UK police forces, Police Scotland does use retrospective facial recognition (RFR), with **reports** that the number of retrospective searches it conducts on the Police National Database have increased in recent years. New **reporting** suggests their approach to LFR might be changing however, with the force apparently considering trials of the technology.

Northern Ireland

Like Scotland, the Police Service of Northern Ireland (PSNI) has taken a more conservative approach to FR than we've seen in England and Wales. Its policies can mostly be deduced from a series of Freedom of Information requests. One from 2020 **stated** that PSNI had not used any Clearview AI products and that it had "not procured or implemented any facial recognition systems". A 2022 request **confirmed** that PSNI does use RFR via the Police National Database. It has used that face-matching service since November 2021, according to a **document** published in 2023. Just like Scotland, there have been no examples of any LFR use.

France

In the run-up to this year's Paris Olympic Games, there was a contentious debate about whether the French police would use LFR. In 2023, the French Parliament approved a new law to enable trials of various security tools at the Olympics. As Reuters have **reported**, this includes 'AI-powered surveillance' to detect specific categories of event, including "crowd surges; abnormally heavy crowds; abandoned objects; presence or use of weapons; a person on the ground; a fire breaking out; contravention of rules on traffic direction". Ultimately, this appears to be analysis of surveillance camera footage, but not LFR; there's no provision to identify wanted individuals in real-time through facial matching.



Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

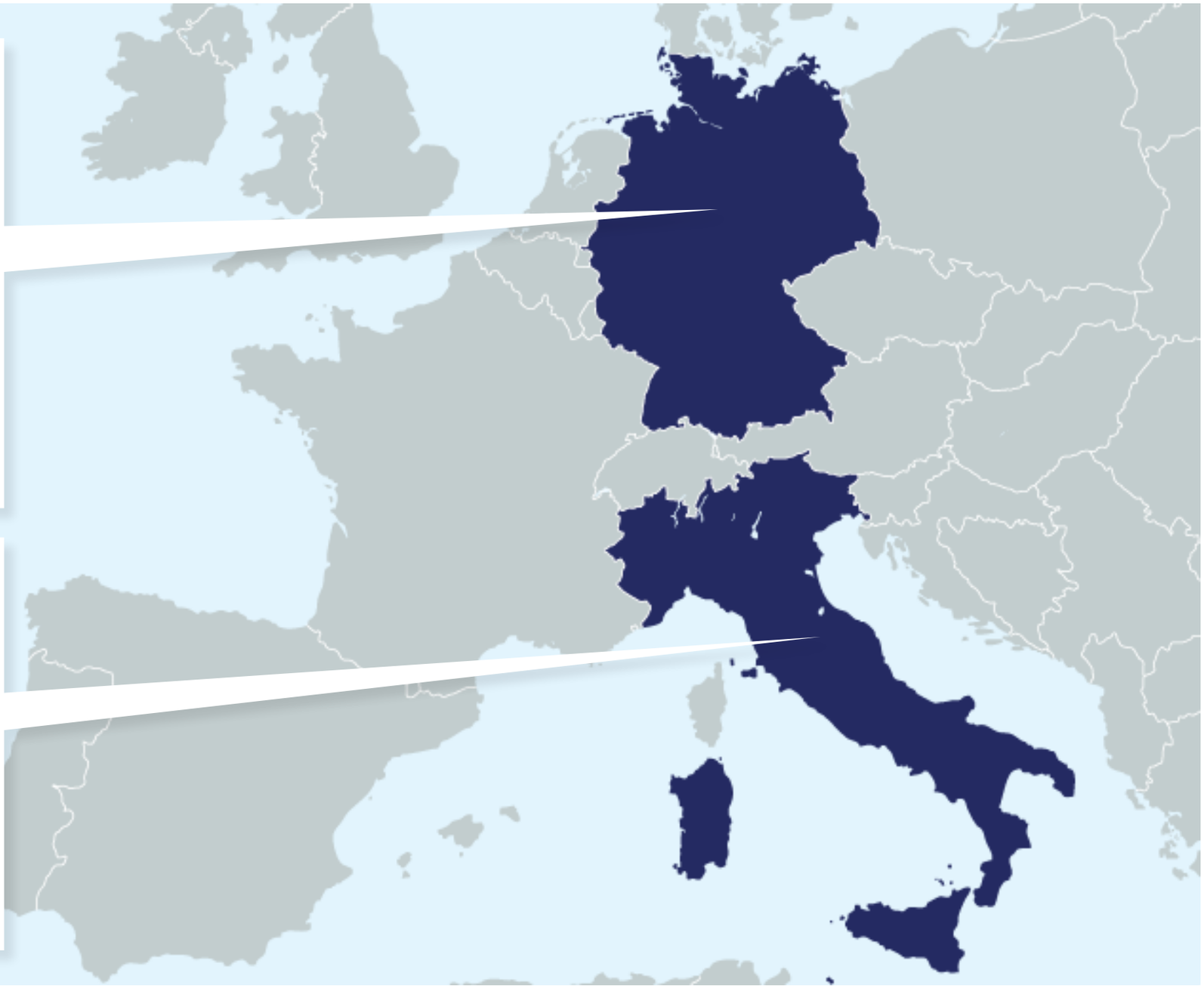
Facial recognition around the world

Germany

In Germany, some limited trials of LFR have taken place. In 2018, the police ran **a trial** at Berlin Südkreuz station, where 300 volunteers (paid €25 each) were placed on a watchlist to test an LFR system. Further limited testing, including of object detection cameras, was also completed in the years after that and more recent **reporting** shows that limited LFR trials are still taking place in a very few areas. RFR is commonplace. Since 2008, the **Federal Criminal Police Office** has allowed all state and federal police to access RFR. This capability compares suspect images against the nation's Inpol database, which has over 7 million images of over 5 million people. In 2022, 2,853 unknown people **were identified** through this system.

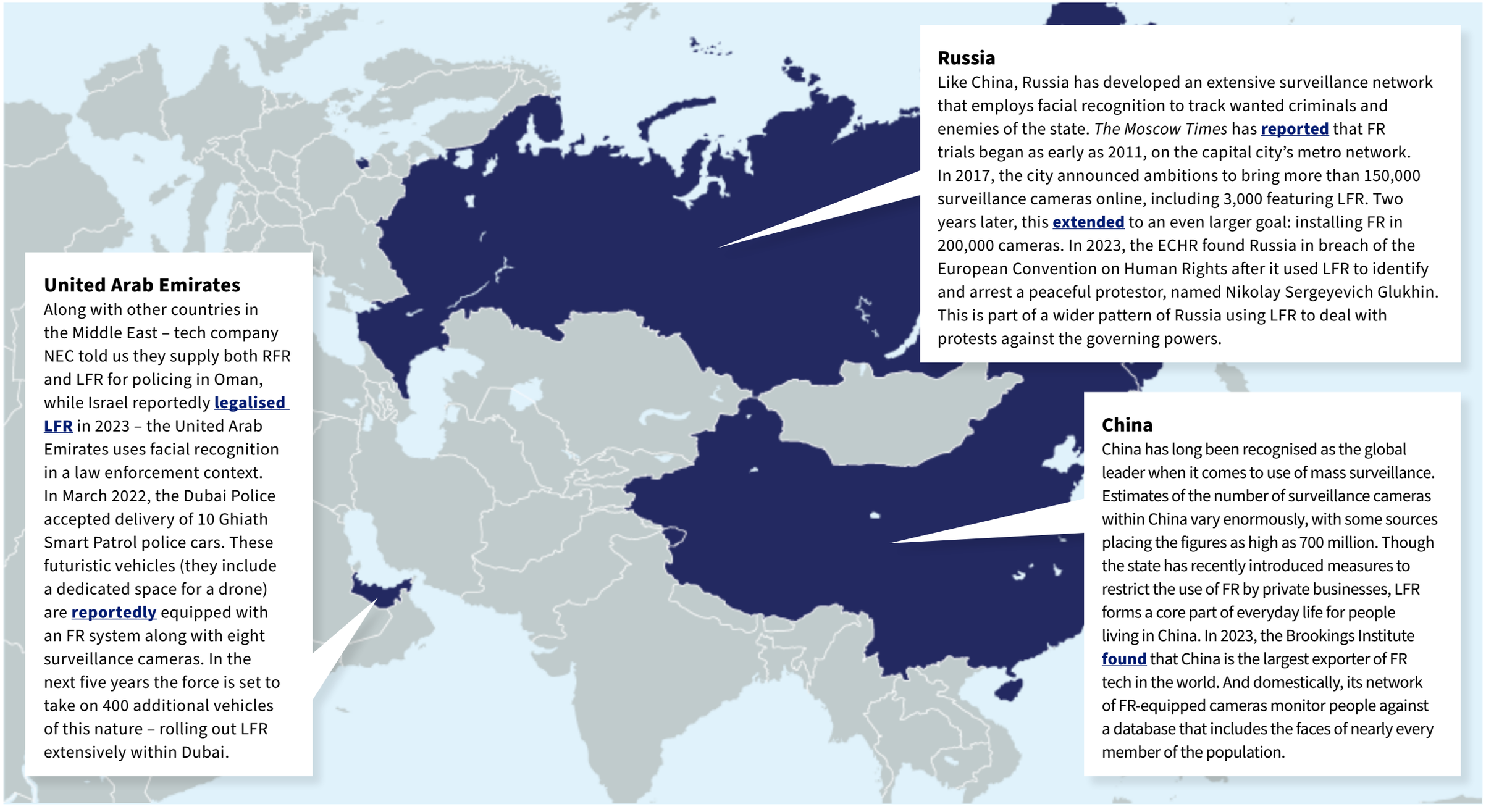
Italy

In 2021, Italy's Data Protection Authority made headlines when it **pre-emptively banned** the SARI Real-Time system, an LFR product purchased by the Italian Police in 2017. By the time the regulator had issued its opinion, the system had still not been used by the Italian Police. It found that "the system as currently designed would enable mass/blanket surveillance" and "lack[ed] a legal basis to legitimise the automated processing of biometric data for FR in security applications". No LFR system has yet been used operationally by the Italian Police. And as of 2022, the Data Protection Authority also **banned** the use of FR tech altogether – except if it's used to help tackle crime.



Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition around the world



United Arab Emirates

Along with other countries in the Middle East – tech company NEC told us they supply both RFR and LFR for policing in Oman, while Israel reportedly **legalised LFR** in 2023 – the United Arab Emirates uses facial recognition in a law enforcement context. In March 2022, the Dubai Police accepted delivery of 10 Ghiath Smart Patrol police cars. These futuristic vehicles (they include a dedicated space for a drone) are **reportedly** equipped with an FR system along with eight surveillance cameras. In the next five years the force is set to take on 400 additional vehicles of this nature – rolling out LFR extensively within Dubai.

Russia

Like China, Russia has developed an extensive surveillance network that employs facial recognition to track wanted criminals and enemies of the state. *The Moscow Times* has **reported** that FR trials began as early as 2011, on the capital city's metro network. In 2017, the city announced ambitions to bring more than 150,000 surveillance cameras online, including 3,000 featuring LFR. Two years later, this **extended** to an even larger goal: installing FR in 200,000 cameras. In 2023, the ECHR found Russia in breach of the European Convention on Human Rights after it used LFR to identify and arrest a peaceful protestor, named Nikolay Sergeyevich Glukhin. This is part of a wider pattern of Russia using LFR to deal with protests against the governing powers.

China

China has long been recognised as the global leader when it comes to use of mass surveillance. Estimates of the number of surveillance cameras within China vary enormously, with some sources placing the figures as high as 700 million. Though the state has recently introduced measures to restrict the use of FR by private businesses, LFR forms a core part of everyday life for people living in China. In 2023, the Brookings Institute **found** that China is the largest exporter of FR tech in the world. And domestically, its network of FR-equipped cameras monitor people against a database that includes the faces of nearly every member of the population.

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Facial recognition around the world



Brazil

Brazil has experimented with LFR for public safety purposes. São Paulo's annual carnival plays host to around 15 million people every year – it's recognised as the largest on the planet by **Guinness World Records**. Since 2020, the local Civil Police have **deployed LFR** at this enormous event, something London's Met Police also **trialled** at the Notting Hill Carnival in 2017. This practice appears to have continued, with **news stories** revealing that LFR has been used at this year's Carnival once again.

Argentina

Argentina's capital, Buenos Aires, has been the site of a long-standing legal battle over the use of LFR, and one that shows no signs of abating. According to a **Chatham House report**, security forces frequently used LFR cameras (including at transport hubs) from 2019 onwards, until an April 2022 court order saw this surveillance suspended. While law enforcement claimed it had been effective at finding wanted people, a judge **raised concerns** after finding that politicians, journalists and campaigners appeared to be on the database. This ruling was effectively upheld in February 2024, when a new court **concluded** that the LFR system could only be used again once a clear audit process had agreed. At the time of writing, that's not been put in place

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

3

The big debates

The big debates Stakeholder voices



"Our concept of privacy in public spaces has not kept up with changes in technology. The traditional position has been that if you're out in public, then apart from situations where you might be getting changed or doing something private, you're fair game… A lot of our search and surveillance laws are based on these outdated ideas."

Dr Nessa Lynch
Matheson Lecturer in Law, Innovation & Technology, University College Cork

"Our philosophy is summed up by a 'computer-in-the-loop' approach. You'll have heard of human in the loop of course, where somebody is overseeing what the machine is doing. In our case, the machine is purely there in the loop of a human, an accountable, identifiable member of the force."

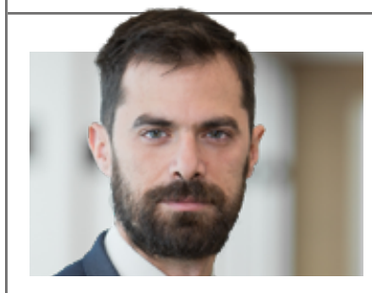
Andrew O'Sullivan
Chief Information Officer,
An Garda Síochána



"It's really important not to insert humans into the loop to just confirm or amplify the results of the FR system. Humans must be there to ensure there's a level of scrutiny that can pick up on false positives, systemic trends, and discrimination or bias."

Patricia Kosseim
Information and Privacy Commissioner of Ontario





"FR has a chilling effect on anyone who might think: 'Oh, I don't want to be there in the public space when it's being used.' This isn't measurable, it's intangible… The assumption that there will be this chilling effect is something that the courts don't have difficulty in accepting."

Professor Kyriakos Kotsoglou
Associate Professor, Northumbria Law School

"It's about who developed the algorithm. We had a very smart Indian-American professor who helped develop algorithms in India. And it happens that, if Asian people develop the algorithm, you have better identification of that group. It's basically down to the developers' bias. You need to knock that out to use the tech properly."

Ira Reese
CTO,
Global Security Innovative Strategies





"The problem is that the tech is presented as offering an objective, neutral space. But it turns out the tech itself is inherently biased. That's because it was designed by biased humans and fed with selective datasets that reflect human bias too."

Dr Elizabeth Farries
Co-Director, UCD Centre for Digital Policy

"There's the evolution of the algorithm from [being able to recognise people] face-on and with a nice clear picture, to now where we're getting matches from some images that are fuzzy, black-and-white, or side-on."

Stuart Moss
Sales Director for Public Safety,
NEC Software Solutions

"We end up allowing litigation to write policy. Any lawyer will tell you that litigation is probably the most expensive, least predictable, and least flexible way of deriving policy. All it does actually – whether win, lose or draw – is undermine public confidence if they constantly see police chiefs being brought into court."

Fraser Sampson
Professor in Governance and National Security,
Sheffield Hallam University



Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

The operational value of FR

Although facial recognition is often described as making a significant difference to public safety, the specific benefits it offers aren't always clear. We spoke to police leaders to understand exactly how FR is a useful tool in policing's arsenal.



For both the police and politicians in England and Wales, there's a high level of confidence that facial recognition (FR) can have a transformative impact. **Policing Minister Chris Philp told Policing Insight** in January 2024: "The increased use of facial recognition (FR) – both live and retrospective – can transform policing and dramatically increase the number of criminals that get caught." At a Conservative Party Conference fringe meeting last year, **LBC reported** that he'd called retrospective facial recognition (RFR) "game-changing" in helping the police identify wanted offenders.

From the police side, Lindsey Chiswick, the Met's Director of Intelligence and the NPCC Lead for Facial Recognition, has **described FR in similar terms**. She called it a "game-changer", arguing that "it's the biggest development in policing since DNA or fingerprints".

When it comes to live facial recognition (LFR) deployments specifically, both the Met and South Wales Police argue that they are highly targeted and focus on crime problems highlighted by an 'intelligence case'. The Met creates tailored watchlists for each individual deployment based on this intelligence, there's no single watchlist used the entire time.

Ms Chiswick recently added more detail on this intelligence-led approach **during testimony to the Justice and Home Affairs Committee**. She said: "The deployment in Croydon was to tackle serious and violent crime. This year, Croydon has the highest murder rate. It has the highest number of knife crime-related offences. It has a blossoming night-time economy, and with that comes problems such as violence against women and girls. That was the intelligence case that sits behind why we wanted to deploy there."

> **"The deployment in Croydon was to tackle serious and violent crime. This year, Croydon has the highest murder rate. It has the highest number of knife crime-related offences. It has a blossoming night-time economy, and with that comes problems such as violence against women and girls."**
>
> **Lindsey Chiswick, Director of Intelligence, Met Police, and NPCC Lead on Facial Recognition**

However, the overarching goals of each Met deployment are relatively static. In fact, **every deployment in 2023 and 2024** has had the same stated purposes, coded as '1,2,3,4' each time. In basic terms, these codes refer to locating people: (1) suspected of committing or about to commit a crime, (2) wanted by courts and with an outstanding warrant, (3) at risk of harming themselves or others, and (4) subject to various legal conditions that are at risk of being breached.

Enforcement and deterrence

The Met's list gives us some sense of what LFR deployments are intended for, but it's closer to a typology of targets than a set of strategic goals; it's important therefore to explore what those goals might be.

First, there's straightforward enforcement. A wanted person – whether by the police as a suspect, or by courts for non-appearance – is flagged up by the LFR system and (sometimes) arrested. This is the simplest benefit and the one the public are probably most conscious of.

The LFR system's real value here is its ability to identify people better than humans can. That's partly because the best algorithms are simply

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

better than the average person at spotting faces. But it's also about both 'breadth' and 'depth' of memory. A machine can 'remember' many more faces than a human can and that ability is not reliant on 'seeing' the face recently. Hence the **Policing Minister's oft-cited case** of the person flagged up by LFR who was wanted since 2015.

This benefit is tough to deny; LFR can certainly spot wanted people effectively and it's better at it than humans. The algorithms will continue to improve rapidly too, while humans' abilities aren't going to advance. The real question (which we'll address later in this chapter) is about proportionality. What types of offenders or crime types should police be able to target with LFR?

Secondly, there's a deterrence angle. This is the idea that LFR deployments will discourage dangerous or disorderly people from being somewhere at a specific time. Of course, this only applies under the current police approach of using overt LFR, advertised in advance.

There are a few high-profile examples of this. Former PCC Alun Michael suggested that even the very first South Wales LFR deployment (which had very poor accuracy) "worked pretty well as a preventative measure to deal with ticket touting… a problem that had dogged previous Champions League finals". He also pointed to its use at major music events to prevent sex offenders entering the area. In Northamptonshire, the force's first LFR usage at the British Grand Prix was partly to deter Just Stop Oil activists who'd previously disrupted the event.

The challenge is that deterrence is difficult to measure. Prof Paul Taylor, UK Chief Scientific Adviser for Policing, told us: "When it comes to LFR, we can't really do a comparison, because we're not allowed to run it without pre-warning people that we're using it. And that would technically be the control group, wouldn't it? Doing it while no-one knew it was there vs doing it while people know it's there… I think it's almost impossible from a science perspective to get the 'delta difference' on prevention. But there's a lot of anecdotal and qualitative evidence that people find it preventative."



Crime and non-crime benefits

But these aren't the only benefits. There's a somewhat contestable reassurance point. As Prof Taylor put it: "There's assurance to the public too… The police have deployed LFR at music festivals before. If I'm sending my daughter there and I know the watchlist is taking out major drug dealers, I actually find it quite reassuring that the drug supply will be less there."

This could be extended further. If the police are running LFR at public transport hubs or night-time venues to identify people wanted for VAWG offences, do those places feel safer for women? On the other hand, for those who don't trust the police or have been unfairly stopped in the past, LFR could have the opposite effect. Do those places become no-go zones for people who fear police attention, even if they aren't on any watchlist?



Linked to this is an enforcement-adjacent benefit around compliance. The Met regularly uses LFR to identify and engage with people who have legal restrictions of various kinds (such as sex offenders). This is 'purpose 4' in their deployment records. LFR might ensure these potentially dangerous people are more regularly checked for compliance with court or police restrictions. If someone was stopped at the train station every day as they headed to work, that might seem disproportionate. But a more proportionate approach could still offer more regular scrutiny and catch bail breaches (or similar) that threaten public safety.

One final potential benefit relates to policing's non-crime work – how LFR can help identify missing people or those with mental health issues. South Wales Police Inspector Karl Roberts offered a personal example of this during an interview. "My [family member] hasn't got the skills and ability to make themself known to policing. But if they walked past an LFR camera and were a missing person, it would identify them and allow the engagement team to give support. And certainly in South Wales, we use LFR's capability to locate and trace vulnerable and at-risk people. That's something I would like publicised a little bit more. LFR is not just about identifying the bad guys and girls."

> **"My [family member] hasn't got the skills and ability to make themself known to policing. But if they walked past an LFR camera and were a missing person, it would identify them and allow the engagement team to give support. And certainly in South Wales, we use LFR's capability to locate and trace vulnerable and at-risk people. "**
>
> **Insp Karl Roberts, South Wales Police**

Continued overleaf

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

A scenario where missing people – including those who are long-term missing – are included on every police LFR watchlist would offer one obvious way to make finding them just a little easier. As Insp Roberts points out, the LFR debate doesn't often focus on this type of benefit, but it might make the difference if someone is finally found.

No final verdict

For all these potential benefits, there remains a question about how deep the impact of LFR is, and how much more effective policing is with this tool. As we noted earlier, Lindsey Chiswick has argued that LFR does help with this: "If you took the same 12-18 uniformed officers on the street without that tech, they'd have nothing like the success the [LFR] has."

Others still think the risks outweigh these upsides. Dr Nessa Lynch, Matheson Lecturer in Law, Innovation & Technology, University College Cork, told us: "I haven't personally seen what you would provide if you're writing a business case to adopt the LFR technology. What is that hard evidence that it would achieve law enforcement objectives which would outweigh the problems that it would bring?"

> **"I haven't personally seen what you would provide if you're writing a business case to adopt the LFR technology. What is that hard evidence that it would achieve law enforcement objectives which would outweigh the problems that it would bring?"**
>
> **Dr Nessa Lynch, University College Cork**

It's also true that future LFR systems could offer more advanced opportunities. We've already highlighted one interviewee's claim that FR systems have been used to protect Taylor Swift from stalkers. Could a future police LFR system work to protect people at a more granular level? For example, could it raise the alarm if a stalking victim (who's opted in to this scheme) and their stalker pass by the camera in a similar time window? These are beyond the reach of the police's current approach, but might not be in a few years' time.

RFR and OIFR

Although LFR is our main focus throughout this chapter, it's important not to forget the purported benefits of retrospective facial recognition (RFR) and operator-initiated facial recognition (OIFR) too.

With RFR, the goal is simply to identify someone from an image you already have. One advantage of using FR for this task is that it's faster. The Home Office points to a **police study** which found that: "Without RFR, identifications take around 14 days, whereas with it they typically take minutes."

FR can help with bulk tasks too, with the ability to review hours of CCTV footage and pull out faces (for example) far more quickly than a human can, as Stuart Moss, NEC's Sales Director for Public Safety pointed out. And it's also more accurate than humans, meaning that FR offers a higher chance of a match than the average officer sorting through a list of faces manually. Because of all this, there's much less criticism of RFR than LFR. It's not surveillance, so it's less privacy-intrusive. Even groups like Big Brother Watch don't call for an outright ban on police RFR.

What is perhaps more controversial is when non-police databases are used for RFR searches. In the context of Ireland, Dr Lynch told Policing Insight: "I would hold enormous concerns about police having a reference database for FR which includes people who have no connection to the criminal justice system, such as images taken from the passport system or a driving licence."

In England and Wales, Liberty Investigates found that **police have been using UK passport databases** to identify people through RFR since at least 2019. That raises fears that data is being used in ways the public never expected and, therefore, might be more inclined to disapprove of.

Finally, OIFR is still at relatively early stages, though the Home Office claims it's "showing positive results". Again, the benefits are essentially speed and accuracy – officers can identify individuals more often and more quickly at incidents. This would help them respond more appropriately, especially where an indvidual is not capable of giving their details (due to injury or mental health issues). The NPCC is set to **roll out OIFR more widely**, so that it's available to all forces in England and Wales sometime this year.

CLICK HERE
Article
Policing Minister urges UK forces to 'dramatically and urgently' increase use of facial recognition
Chris Philp wants to dramatically increasing the use of FR
policinginsight.com

CLICK HERE
Article
How facial recognition technology has changed policing
Scanning tool is the biggest game-changer for officers since DNA
thetimes.co.uk

CLICK HERE
Report
Corrected oral evidence: Live facial recognition
Transcript of evidence taken in public
committees.parliament.uk

CLICK HERE
Report
MPS LFR deployments 2023-date
Data from the Metropolitain Police on live facial recognition deployments
met.police.uk

CLICK HERE
Report
Police use of Facial Recognition: Factsheet
Home Office factsheet on police use of facial recognition technology
homeofficemedia.blog.gov.uk

CLICK HERE
Report
Police secretly conducting facial recognition searches of passport database
Hundreds of secret facial recognition searches conducted
libertyinvestigates.org.uk

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Biased systems or accurate tools?

Discussions around bias and accuracy are central to the facial recognition debate and are a common reason for some people's opposition to police use of this technology, especially in a live setting.



At the heart of the facial recognition (FR) debate are concerns about bias and accuracy. Even if FR really does offer significant operational benefits, there's a fear that the tech just can't be trusted. In reality, AI isn't and can't ever be 'neutral'. It's intrinsically biased in ways we should be deeply worried about, especially in the high-risk context of enforcing the law.

It's for this reason that many remain opposed to the police use of FR, especially live facial recognition (LFR). Claims about its accuracy remain hotly contested by those on either side. Even studies such as the **2023 National Physical Laboratory (NPL) report** (which evaluated the FR algorithms used by police in England and Wales) haven't convinced the doubters.

Biased creators, biased products

The FR debate reflects a broader fear about any police use of AI tools. The danger is that, by using notionally 'neutral' AI products, police decisions can be framed as 'unbiased' – even when they're far from it.

Dr Elizabeth Farries, Co-Director of the UCD Centre for Digital Policy, told Policing Insight: "The problem is that the tech is presented as offering an objective, neutral space. But it turns out the tech itself is inherently biased. That's because it was designed by biased humans and fed with selective datasets that reflect human bias too."

In a **2020 paper**, Dr David Leslie of the Alan Turing Institute made a similar point about FR: "As these [facial detection and recognition technologies (FDRTs)] became primarily data-driven, their dependence on large-scale datasets spurred new forms of bias. Imbalanced datasets with less representation of marginalised demographic groups would train FDRTs to be less accurate for them."

And there are plenty of examples of biased algorithms. In 2015, the AI tagging software used in **Google's Photos app was found to be labelling Black users as 'gorillas'**. In 2020, Twitter's auto-image cropping algorithm was **reported to edit out darker faces** from pictures in favour of lighter ones.

Related challenges exist with the latest wave of generative AI tools. In 2024, Google's chatbot Gemini **refused to show white people** when asked to produce images of German soldiers in World War 2. Instead, it produced people of colour in all the images, due to well-intentioned pro-diversity settings. Things like the training data or configurations of an AI tool will affect its outcomes, often in unpredictable ways.

> **"The problem is that the tech is presented as offering an objective, neutral space. But it turns out the tech itself is inherently biased. That's because it was designed by biased humans and fed with selective datasets that reflect human bias too."**
>
> **Dr Elizabeth Farries, UCD Centre for Digital Policy**

Worrying cases from the US

When it comes to the police use of FR, critics often point to concerning US cases which, they argue, illustrate the potentially racist outcomes of these tools. As a **2024 report from the National Academies of Sciences, Engineering and Medicine's Committee** on FR notes: "All six known cases where wrongful arrests have been made on the basis of FRT [in the US] involve Black individuals identified using FRT."

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

One case – involving an African-American man named Robert Williams – is presented in detail within the report. After an incident where watches were stolen from a shop, a private company provided Detroit PD with camera footage of the thief. The police department asked Michigan State Police to use RFR to identify him. They, wrongly, alleged Mr Williams was the perpetrator. He was arrested in January 2020 and detained for 30 hours. The charges were later dropped.

Another involved a woman named Porcha Woodruff. The report states: "She was arrested and held for 11 hours in Detroit in 2023 for carjacking and robbery, despite the fact that she was eight months pregnant at the time of the crime and the perpetrator was not."

Clare Garvie, a lawyer with the Fourth Amendment Center and expert on police FR, told Policing Insight that there are "no minimum photo quality standards in the US" for inputting photos in FR systems. That can only increase the risk of bias.

> **"It's about who developed the algorithm. We had a very smart Indian-American professor [on the committee] who helped develop algorithms in India. And it happens that, if Asian people develop the algorithm, you have better identification of that group. It's basically down to the developers' bias. You need to knock that out to use the tech properly."**
>
> **Ira Reese, CTO, Global Security Innovative Strategies**

As it stands, there appear to be no known cases of someone being convicted on the basis of FR alone. And those six US cases don't seem to involve LFR, but retrospective facial recognition (RFR) instead. Some, such as the Williams case, appear to reflect both human and machine error. He was listed as the ninth-likeliest match by one FR algorithm, which two humans later verified. The importance of an effective human in the loop is something we'll return to.

In England and Wales, the experience has been different. Dr Asress Gikay, Senior Lecturer in AI, Disruptive Innovation, and Law at Brunel Law School, has **previously written**: "Despite the UK police using FR for more than six years, there has not been a single reported case of wrongful arrest, contrasted with the US where several incidents have been documented."

Inside the algorithms

Importantly, it's not the case that algorithms are always biased against the same ethnic groups, regardless of where or how they're created. Ira Reese, CTO of Global Security Innovative Strategies, who contributed to the National Academies report, said: "It's about who developed the algorithm. We had a very smart Indian-American professor [on the committee] who helped develop algorithms in India. And it happens that, if Asian people develop the algorithm, you have better identification of that group. It's basically down to the developers' bias. You need to knock that out to use the tech properly."

Dr Andrew Chen, Senior Research Fellow at Koi Tū (the Centre for Informed Futures) at the University of Auckland, concurred. "I think there are some logical inconsistencies [with the idea that the systems are always biased against specific groups]. People say: 'Look at the US systems which don't work very well on Asian faces.' Well, what about China when they use it? If it doesn't work well on Asian faces, they've got a problem. It turns out that the training datasets have a really significant impact on the accuracy and error rates of the outputs."

That's a continuing challenge. But there's broad recognition, even from many sceptics of FR, that the algorithms have become much more accurate over the past decade. There has been some evidence of this with one UK retail-based LFR scheme which has changed its algorithm five times to pursue greater accuracy. And Dr Chen suggested that the poor accuracy figures cited by some FR critics are "probably overstated" and some "are using old numbers" that are out of date.

Of course, it's not as simple as saying all FR algorithms are accurate or inaccurate – there is considerable variance across different manufacturers. The US National Institute of Science and Technology (NIST) produces **regular evaluations** of private firms' FR algorithms. It's widely considered the essential benchmark for measuring the performance of FR systems.

Looking at the **one-to-many facial identification studies** done by NIST, companies such as Cloudwalk, Sensetime and NEC (the dominant provider of police FR in England and Wales) are close to the top, although different tests yield slightly different rankings. This nuanced technical analysis is essential for what is still a relatively unregulated global marketplace.

England and Wales

Looking at a concrete example, the data around the use of LFR in England and Wales suggests that police deployments are proving increasingly accurate here. At **South Wales Police's first LFR deployment** in 2017, there were 2,554 false alerts (against just 173 true alerts). In the approximately 40 deployments between 2023 and the time of writing, there were no false alerts. This partly reflects the force's decision to use the 0.64 threshold setting, a more exacting standard than the default (0.6) within the NEC system. For the Met (which uses the 0.6 setting), its **around 100 deployments in 2023 and 2024** have yielded less than 20 false alerts in total.

Perhaps more revealing is the much-cited 2023 **NPL facial recognition equitability report**. This provided independent testing of the 'NEC Neoface V4 using HD5 Face Detector' system, when used in operational conditions. In other words, it gives a verdict on the algorithms used by policing in England and Wales for LFR, RFR and operator-initiated facial recognition (OIFR) too.

The NPL's results offer much to support policing's case. For RFR and OIFR, it found a 100% true positive rate, meaning every image evaluated by FR returned the correct person as the 'top match'. Of course, with both systems scoring "the best performance possible", there was "no demographic performance variation" either.

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

On LFR, things are more complicated. At the default face-match threshold of 0.6, the true positive rate – how often a wanted person who walks by the LFR camera is correctly identified – was 89%. That number was the same whether the police watchlists consisted of 1,000 or 10,000 people. The false positive rate – how often an innocent person was incorrectly identified as 'wanted' by the LFR system – varied. For watchlists of 1,000 people, 1 in 60,000 people walking by were falsely flagged. For watchlists of 10,000 people, this was higher: 1 in 6,000 would be falsely identified. The Met claims that, based on data from recent deployments, false positives are proving even less common than this.

> **"My personal opinion, when it comes to bias, is that if it's not already solved, it will be solved in the next three to five years. I think the bias issue is probably overstated and it's an unreliable argument for the civil liberties groups, because it will go away at some point."**
>
> **Dr Andrew Chen, Senior Research Fellow, University of Auckland**

On the question of bias, the evaluation reported a nuanced set of results. At the default 0.6 face-match threshold used by the Met, there was no statistically significant gender or racial bias for either true positives or false positives. That's with the exception of age where, interestingly, a higher true positive rate was found for those aged 42+ (at 93%), versus 20-41s (89%) and under-20s (83%).

However, bias can become evident at different settings. If you increase the threshold to 0.64 (the approach used in South Wales), there were no false positives at all – so statistical bias on this metric is entirely absent. At the 0.62 and 0.6 levels, there were one and seven false positives respectively, although these didn't show any statistically significant demographic bias. The problem comes lower down, at the 0.58 and 0.56 settings. At these levels, the NPL report explains, false positives "start to show a statistically significant imbalance between demographics, with more Black subjects having a false positive than Asian or White subjects."



Or to put it simply:

- At the 0.6 setting the police's LFR system from NEC wasn't biased – except for age.
- At 0.62 and 0.64, false positives more or less disappear – though the true positive rate drops too; there were fewer hits overall and, in turn, fewer false IDs.
- At 0.58 and 0.56, the false positive rate jumps up, meaning more innocent people are wrongly flagged up – and this problem disproportionately affects Black people.

Mixed verdicts

The study was understandably welcomed by policing. **In a statement** (since deleted from the Met website), the force's Director of Intelligence and NPCC Lead for FR, Lindsey Chiswick, said: "This research means we better understand the performance of our algorithm. We understand how we can operate to ensure the performance across race and gender is equal."

NEC itself unsurprisingly agrees with this perspective too. In an interview with Policing Insight, NEC's Sales Director for Public Safety, Stuart Moss, pointed to the NPL report as evidence that the algorithm could be trusted. He also stressed the improving accuracy of FR systems: "There's the evolution of the algorithm from [being able to

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

recognise people] face-on and with a nice clear picture, to now where we're getting matches from some images that are fuzzy, black and white, or side-on." He described the ability of FR algorithms to identify people wearing masks as further evidence of this.

The algorithms used in FR have improved rapidly and are expected to keep doing so. Dr Chen said: "My personal opinion, when it comes to bias, is that if it's not already solved, it will be solved in the next three to five years. I think the bias issue is probably overstated and it's an unreliable argument for the civil liberties groups, because it will go away at some point."

For now though, there's still some level of scepticism. Madeleine Stone, Senior Advocacy Officer at Big Brother Watch, argued in an interview: "That report obviously found that the tech did have statistically significant bias – it just found that at certain thresholds that bias is no longer visible. We've compared it to if you had a self-driving car and said, for example: 'Well, it's safe if you drive at 20 miles per hour.'"

> **"[With FR], you're overlaying another technology and tactical option into an already institutionally racist system with disproportionality against Black people across the board. [There's bias around] Taser usage, stop and search, use of force, death in custody."**
>
> **Andy George, President, National Black Police Association**

Beyond technical solutions alone

The NPL testing has clearly moved the debate forward, at least in England and Wales. It proves that policing's current LFR systems show no racial bias at 0.6 (or above). That's an important piece of evidence.

However, the 0.6 level isn't set in stone. The police accept that they would drop below this setting in specific, narrow circumstances. In an interview, Ms Chiswick pointed to a terrorist attack as one case where it might be reasonable to drop the threshold. That might seem proportionate, but it runs into another challenge with FR.

As there's no single piece of legislation, the 0.6 level isn't legally mandated. There isn't a list of specific circumstances under which policing is permitted to drop below 0.6. Even the **College of Policing's authorised professional practice on LFR** doesn't refer to this level. And we've seen divergent approaches already. South Wales uses 0.64, while the Met uses 0.6 with the same NEC algorithm. Many of the stronger arguments against LFR are therefore more concerning because there's so little external oversight. We're relying on policing's own guidance to ensure good practice, not legislation or external regulation in many cases.

However, there's a second challenge here too. A broader, more complex and contested one, that isn't really about technology at all. It's about the wider context of how policing operates in different communities and the confidence (or lack of it) across different parts of society.

As Andy George, President of the National Black Police Association argues: "[With FR], you're overlaying another technology and tactical option into an already institutionally racist system with disproportionality against Black people across the board. [There's bias around] Taser usage, stop and search, use of force, death in custody."

So even if the narrow question of bias in the algorithm is addressed, whether by sticking at 0.6 or developing even more accurate algorithms in the future, this wider issue will remain. The perennial policing challenges – trying to protect but not over-police, building confidence while tackling a legacy of distrust – won't be solved with a shiny new algorithm. Where and how LFR is used in communities will be just as important as the system sitting behind the camera lens.

CLICK HERE
Report
Facial recognition technology in law enforcement equitability study
Results of an evaluation of facial recognition technology
science.police.uk

CLICK HERE
Report
Understanding bias in facial recognition technologies
Explanatory report on bias
turing.ac.uk

CLICK HERE
Report
Facial Recognition Technology
Current Capabilities, Future Prospects, and Governance
nap.nationalacademies.org

CLICK HERE
Report
Face Technology Evaluations - FRTE/FATE
Evaluation of face recognition and analysis technology
nist.gov

CLICK HERE
Report
Face Recognition Technology Evaluation (FRTE)
False Negative Identification Rates
pages.nist.gov

CLICK HERE
Report
Deployments for Live Facial Recognition
South Wales Police deployed live facial recognition in Swansea City Stadium
south-wales.police.uk

CLICK HERE
Report
MPS LFR deployments 2023-date
Data from the Metropolitain Police on live facial recognition deployments
met.police.uk

CLICK HERE
Article
Statement on release of research into FR technology
Met says it will use FR as a first, but significant, step towards precise community-based crime fighting.
web.archive.org

CLICK HERE
Policy
Live facial recognition
Guidance for the overt deployment of live facial recognition (LFR) technology
college.police.uk

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

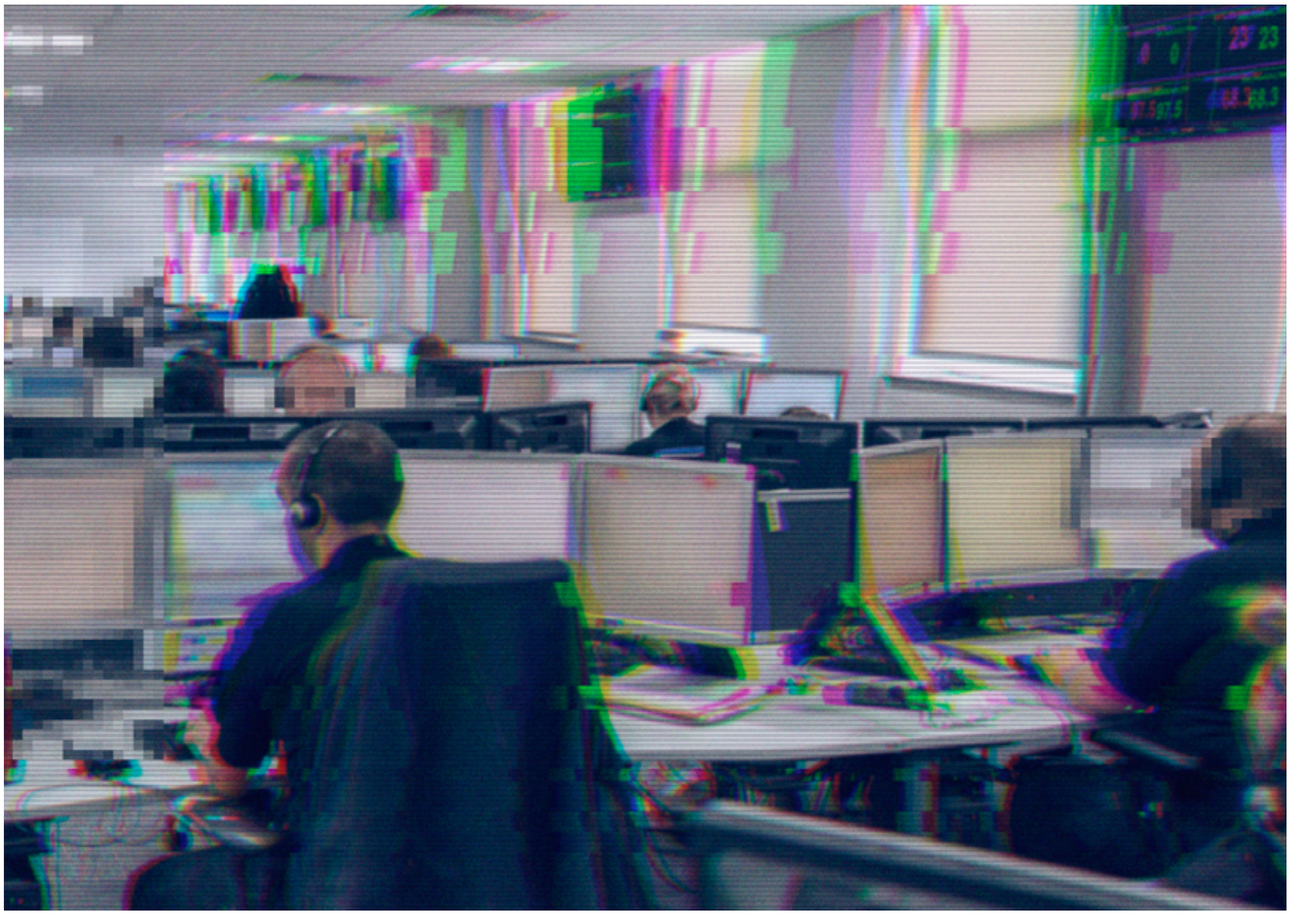
The human in the loop

Human involvement in overseeing any FR system is often seen as an essential requirement for a trustworthy use of this technology. But does the human presence really reduce bias?

Policing is often defined – on the frontline at least – by its physicality. The right to chase, detain, arrest, and sometimes imprison a person is central to what makes it distinct from many other public services. Even as cybercrime and new technologies challenge that narrative, it remains true that policing is distinctly grounded and deeply human.

Facial recognition (FR) is, surprisingly, no exception to this. Yes, it uses AI to identify a suspect, but actioning that intelligence still requires the usual human response. And even this identification process is inextricable from its human inputs.

Humans create the watchlists, humans decide where and for how long live facial recognition (LFR) is deployed, and humans still play, in most cases at least, a central role in verifying the matches an FR system throws up. This last idea, often described as having 'a human in the loop', is seen by many as an essential component for a trustworthy and reliable use of LFR. But does the human presence actually reduce bias? And will police officers really challenge a machine they've been told is 'game-changing'?



The computer in the loop

In every one of our interviews with police representatives, they've been keen to emphasise how crucial humans are in their use of FR. And there are different models used in different jurisdictions.

Previously in this report we've explored how, in the Netherlands, the police's Centre for Biometrics integrates human experts when it uses retrospective facial recognition (RFR). The Dutch Police's Lead Specialist on Biometrics, Chief Inspector John Riemen, stressed that the approach has "humans in the loop to make decisions".

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

The algorithm produces a list of possible matches, with a human expert confirming ones they believe are true. This then goes to two other humans for further verification, before being shared with an investigation team. It's a clear example of a highly human-centric system.

In Ireland, An Garda Síochána's Chief Information Officer Andrew O'Sullivan discussed a similar mindset. He said: "Our philosophy is summed up by a 'computer-in-the-loop' approach. You'll have heard of human in the loop of course, where somebody is overseeing what the machine is doing. In our case, the machine is purely there in the loop of a human, an accountable, identifiable member of the force. They are making a decision or deciding what to do with it, [they're choosing whether] to include it or exclude it in their thinking."

This even extends to how speeding tickets are issued, he explained. "As a matter of policy, we don't use any form of automated machine decision making. For example, even our speed cameras do not automatically issue tickets. All they do is indicate that an offence may have taken place.

"It's then reviewed by three people who determine: 'Is the 'read' on the number plate accurate?' It isn't always [accurate] with ANPR; it usually is, but not always. And then they look at other considerations before they decide to issue them with the ticket."

This human-first approach provides clarity in the court process too, said CIO O'Sullivan. "It helps us with the law because we don't get into this debate around 'who made the decision?' It's always the person standing in front of the judge and jury. It's that person standing over their decision."

In England and Wales, things are a little different, although again there's a human in the FR process. At an LFR deployment, when the system produces a possible match, human operators within the van review the captured face against the watchlist. If they agree and confirm the match, uniformed police officers will go and stop the person the system has identified.

> **"Our philosophy is summed up by a 'computer-in-the-loop' approach. You'll have heard of human in the loop of course, where somebody is overseeing what the machine is doing. In our case, the machine is purely there in the loop of a human, an accountable, identifiable member of the force. They are making a decision or deciding what to do with it, [they're choosing whether] to include it or exclude it in their thinking."**
>
> **Andrew O'Sullivan, Chief Information Officer, An Garda Síochána**

The case for humans in the loop

Placing humans within the FR process is partly about public trust. Rather than relying on a technology some might feel hasn't been sufficiently tested or which remains new and concerning, adding a human into the loop provides some reassurance. It can defuse concerns about giving too much power to an AI system, especially in the context of policing.

Of course, there are other reasons for this too. Some make the case that human-AI FR systems are ultimately more accurate than using the algorithm alone. While FR technology has become increasingly effective, human oversight provides a way to avoid unnecessary mistakes. Anyone who's experimented with the new wave of generative AI tools knows that they can be incredibly powerful, but occasionally prone to strange or child-like mistakes.

Baroness Sally Hamwee, former Chair of the Lords Justice and Home Affairs Committee, gave a good example of this from her own experience. "I remember a few years ago not being able to get through the gates at the Gare du Nord for the Eurostar. It was because I was wearing earrings which I hadn't been wearing for my passport photo… One of the security people said: 'Take off your earrings', and then it worked!" These errors can creep into AI systems, but basic human intervention – a helping of common sense – can easily overcome them.

Another argument is more legal and practical. In every country across the Western world, police officers and others involved in the criminal justice system face strict rules around what they can and can't do during an investigation. This is designed to limit their power in accordance with human rights and ensure there's true accountability for what can be life-changing decisions.

Relying on an automated decision alone can be illegal or prohibited in some cases. At the very least, it can provide a persuasive means for a defendant to challenge the evidence against them – whether lawful or not. A jury may not trust the outcome of a computer system 'acting alone', no matter how advanced the algorithm it uses.

Back to bias

The final and most contentious argument takes us back to bias. Does including humans in the FR process reduce or increase the risk of discrimination? As a **report from the Alan Turing Institute** on biometrics points out: "Mitigating demographic bias is particularly critical in law enforcement… given the potential impact on individuals' human rights."

It continues: "Bias can also be introduced by humans in the loop (operators using the system) which can be more difficult to test and detect." The black box phenomenon isn't constrained to robots alone.

It's clear that understanding the influence of human bias can be

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

tricky. And while the LFR system used in England and Wales has performed well when tested for bias at default settings, other FR systems aren't necessarily so reliable. Is it perhaps that the humans don't cancel out bias, but reinforce it?

As Dr Elizabeth Farries, Co-Director of the UCD Centre for Digital Policy, put it: "Tech is often presented as objective and neutral, but it's inherently biased. Things like facial recognition were designed by biased humans and fed with selective data informed by those biases.

"The human-in-the-loop argument suggests that humans can somehow solve that problem. But if you've got police forces with histories of discriminatory practice, putting their potentially biased agents into a biased technological process doesn't solve that problem. Indeed, it can exacerbate it."

There's a slightly different risk around bias too. Rather than reinforcing biased systems with their own preconceptions, there's a danger that the human in the loop isn't doing much at all. They simply follow what the machine tells them is the right answer.

Clare Garvie, a lawyer with the Fourth Amendment Center and expert on police FR, explained: "There's still a problem if the system returns possible matches and the human analyst knows those are in rank order (from most to least likely matches). There's going to be incredible cognitive bias towards agreeing with the findings, as opposed to performing any sort of independent systematic review."

In the loop or in control?

This concern gets to the heart of the human-in-the-loop debate. Are police officers in the FR loop performing a mere reassurance role, making sure the public know humans are still in control, but ultimately just going along with the FR system every time? Or are they active, empowered agents in the loop, with the skills and the confidence to challenge systems that might be making mistakes?

Patricia Kosseim, Information and Privacy Commissioner of Ontario, pointed to this risk: "It's really important not to insert humans into the loop to just confirm or amplify the results of the FR system. Humans must be there to ensure there's a level of scrutiny that can pick up on false positives, systemic trends, and discrimination or bias. It's about more than just having a human there in the loop for the sake of it."

But that also requires effective training to make sure people know what to look for when holding an oversight role – something that doesn't always happen, as Clare Garvie noted. "In the US, the individuals might not be trained. They're very often not subject to any proficiency evaluation, it's a total unknown.

> **"Tech is often presented as objective and neutral, but it's inherently biased. Things like facial recognition were designed by biased humans and fed with selective data informed by those biases. The human-in-the-loop argument suggests that humans can somehow solve that problem. But if you've got police forces with histories of discriminatory practice, putting their potentially biased agents into a biased technological process doesn't solve that problem. Indeed, it can exacerbate it."**
>
> **Dr Elizabeth Farries, UCD Centre for Digital Policy**

"They might be good or bad at their jobs, we have no idea. We don't look for this, test it or let anyone evaluate [their ability]. The whole process has a lot of room for error and we don't know what that error actually looks like!"

In England and Wales, things are done differently. In the Met and South Wales Police, forces use specific operators who've been trained to use LFR systems. But this is much easier to get right when only a few forces are using the tech. As it develops across England and Wales, adopting a standardised and high-quality approach will become tougher – something we see frequently in our 43-force model.

Challenging the tech

Ultimately, the human in the loop can only offer value if they're genuinely willing to challenge automated systems. In England and Wales, LFR operators receive specialist training, they're familiar with the tech, and they understand it well. But they're also been told that FR systems are a breakthrough on the scale of DNA with tremendous accuracy and power.

The broader culture of law enforcement can exert its own contradictory pressures too. On the one hand, police officers are usually taught to be sceptical, to test and challenge evidence. So perhaps an LFR system that delivers a match will face some reasonable and beneficial scrutiny.

But policing is also highly procedural and hierarchical, and challenging things can be difficult for insiders. Relying on the technology might be more defensible than drawing your own conclusion. And more critical voices would suggest policing will usually have an instinctive bias towards 'pro-arrest' evidence, even if the FR system doesn't quite look right.

All of these considerations reflect judgement calls about policing and its culture. Unlike the debate around narrow accuracy – about whether the tech has statistical bias – the conversation about the human in the loop can't be 'solved'. Instead, we're left with some outstanding questions. Do humans add bias or reinforce it? How likely are they to challenge algorithms or outputs of them? And how can policing train people to be more than 'just' a human in the loop?

CLICK HERE
Report
The Future of Biometric Technology for Policing and Law Enforcement
Exploring the future of biometric technology for UK policing
cetas.turing.ac.uk

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Intrusion and the threat to privacy

In the absence of much legislation around facial recognition, much of the early oversight has come from privacy regulators. The crucial issue of privacy and intrusion goes to the very heart of the FR debate.

One of the strongest criticisms made by those opposed to facial recognition (FR) is that this technology is inherently intrusive. By scanning and analysing something so fundamental to what makes us human – something that identifies us, shows our emotions and feels closer to our sense of self than other biometrics such as fingerprints ever can – FR, especially live facial recognition (LFR), is simply too great an invasion of our privacy. It's not just that we're caught on camera, it's that we're identified in real-time as we walk down the street.

In the absence of significant legislation around FR, much of the early oversight has come from privacy regulators. For example, Patricia Kosseim, Information and Privacy Commissioner of Ontario, told us about guidance her organisation had produced for local police using RFR.

Regulators in some jurisdictions, such as Australia and Sweden, have launched action in response to tools like Clearview AI. The UK's Information Commissioner's Office has investigated numerous uses of FR too.

Policing itself has generally defended FR as being either an extension of existing, widely accepted tools such as CCTV, or even as being less intrusive in some ways. But the crucial question about privacy and intrusion goes to the very heart of the FR debate.

Orwellian intrusion?

The campaign group Big Brother Watch has been the loudest voice raising concerns about privacy intrusion from LFR. Its Senior Advocacy Officer Madeleine Stone described it as: "A mass surveillance tool that turns the streets of Britain into police line-ups and our faces into barcodes."

She challenged the idea that an LFR scan should be seen as less intrusive than a physical interaction with police. "If we had a police officer take a fingerprint scan, DNA sample or check our ID cards every time we walked down the street, people would feel very uncomfortable about this. But it's no different just because it's being done by a camera. Even though you can't physically feel the intrusive nature of it, it's still happening."

Clare Garvie, a lawyer with the US-based Fourth Amendment Center and expert on police FR, noted that privacy considerations are a wider issue than whether any given system is accurate. "From a privacy perspective, both generally and with real-time FR, a better or more accurate system doesn't necessarily fix the broader implications and risks of FR. For example, [that includes] those rights to associate and to anonymity in public."

> **"If we had a police officer take a fingerprint scan, DNA sample or check our ID cards every time we walked down the street, people would feel very uncomfortable about this. But it's no different just because it's being done by a camera. Even though you can't physically feel the intrusive nature of it, it's still happening."**
>
> **Madeleine Stone, Senior Advocacy Officer, Big Brother Watch**

Of course, even retrospective facial recognition (RFR) systems have privacy implications, especially as some police databases aren't always well maintained. For example, in 2021 it was reported that the **Dutch Police had removed 218,000 photos from suspect databases** which shouldn't have been retained.

Similarly, in 2023, then UK Biometrics and Surveillance Camera Commissioner Professor Fraser Sampson **told *the Guardian*** that police forces in England and Wales held over 3 million custody photos of innocent people. He added: "They were challenged in 2012 and a High Court judge said you must get rid of these in months, not years. Eleven years later they've still got them." If innocent faces are on your watchlist or in your database, the tech becomes inevitably more intrusive.

Police perspective

In England and Wales, police representatives are keen to emphasise how their FR systems try to reduce intrusion. Auto-deletion of scanned faces that don't match is a key part of this.

Lindsey Chiswick, Met Director of Intelligence and NPCC Lead for FR, told Policing Insight: "There's a fleeting engagement of a face [with LFR] which is immediately deleted by the technology if you're not wanted. And you go on your way, you wouldn't know [it's scanned you]. It takes literally milliseconds."

UK Chief Scientific Adviser for Policing, Professor Paul Taylor, echoed those comments: "With LFR, we're taking the image and it's instantaneously deleted if you're not on the watchlist." In other words, even though your face is scanned, that material from 'non-matched' people is immediately and permanently removed from police systems.

And in terms of the deployments themselves, forces point

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

to the overt approach they take to deploying LFR. When LFR is used, the police say they're not trying to hide anything. As Chief Superintendent Sean Wilson, the senior officer responsible for the Ealing deployment we attended told us: "I'm going to be quite open about this with the public. I'm telling them we're going to be using it."

As Policing Insight witnessed when we attended that Ealing deployment, there are bright signs placed on lampposts next to deployments and the police publicise LFR use via social media channels. We also saw signs on the LFR van itself stating that this technology was in operation – although this was too small to be read by anyone far from the vehicle.

But Baroness Hamwee, former Chair of the Lords Justice and Home Affairs Committee (which recently published the **results of a 'short investigation'** into the use of LFR by police in England and Wales) questioned whether this public awareness approach goes far enough.

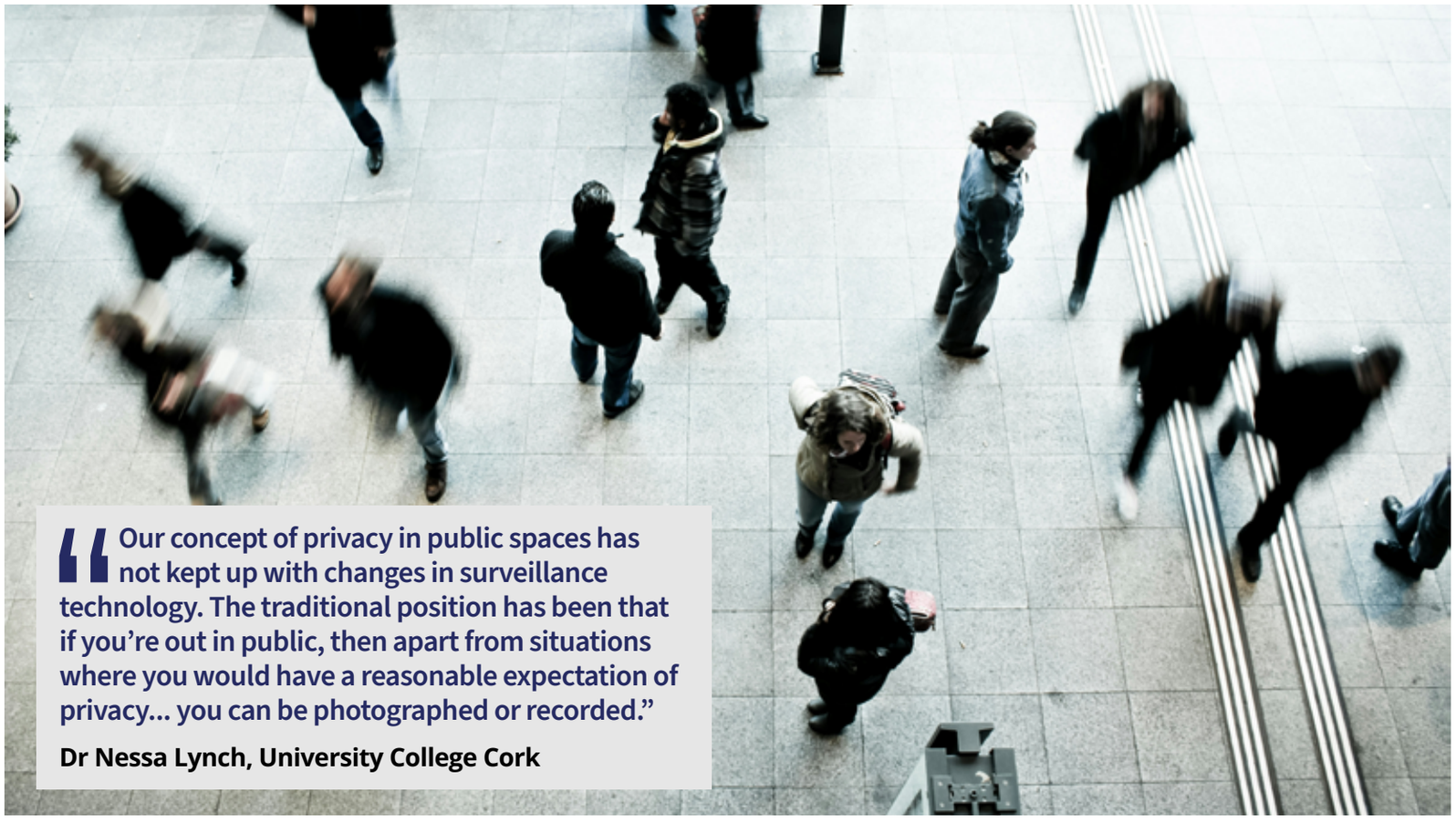
She said: "However much the forces say that they're making it clear to the public that they're deploying the technology, I have no confidence that's obvious to people. The Met, in particular, when they were talking to us, relied on the fact that there is stuff on social media.

"I just don't see that people are going to be coming across it. I'm not a user of social media myself, so perhaps I'm biased. But unless you're in the sector like Big Brother Watch, then you wouldn't be looking for the information."

A scan or a search?

The public's perception of how intrusive an LFR scan is becomes important as a result. Recent polling of UK adults by the **Alan Turing Institute** suggested they broadly support its use. Just 5% wanted biometric systems that identify criminal suspects in crowded areas banned.

Most said they were 'comfortable' with LFR systems used in this way, both in low-diversity areas (61%) and high-diversity areas (60%), and 79% said they trust the police's use of biometrics. The auto-deletion element of LFR would likely be reassuring to many people as well.



> **"Our concept of privacy in public spaces has not kept up with changes in surveillance technology. The traditional position has been that if you're out in public, then apart from situations where you would have a reasonable expectation of privacy... you can be photographed or recorded."**
>
> **Dr Nessa Lynch, University College Cork**

But the concern raised by Big Brother Watch remains important. Is a police scan significantly different to a physical interaction with an officer? Should an LFR scan be legally treated as a police search?

Dr Nessa Lynch, Matheson Lecturer in Law, Innovation & Technology, School of Law, University College Cork, Ireland, expanded on this point. "Our concept of privacy in public spaces has not kept up with changes in surveillance technology. The traditional position has been that if you're out in public, then apart from situations where you would have a reasonable expectation of privacy, such as the situation in Peck v UK where the person was attempting suicide in a public place or where a person is engaged in an activity like getting changed at the beach, you can be photographed or recorded.

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

"But our search and surveillance laws are based on these outdated concepts – a police officer attends a protest, takes one photo of you and does some notations in a notebook. Whereas the tech has moved on massively, and our idea of privacy in the public space hasn't kept pace.

"And there's been discussion in various cases about what the definition of a search is. If you're using a system that's recording and analysing data from you – such as real-time biometric surveillance such as live facial recognition – should that count as a search?"

Dr Elizabeth Farries, Co-Director of the UCD Centre for Digital Policy, made a similar argument, suggesting that surveillance – even with immediate deletion – is still a significant intrusion. "It flies in the face of norms around criminal law to say that someone who's not suspected of a crime should be subject to police surveillance, which is what LFR does. If you're not a suspect, you shouldn't be scanned. That's a fundamental principle of criminal law."

> **"It flies in the face of norms around criminal law to say that someone who's not suspected of a crime should be subject to police surveillance, which is what LFR does. If you're not a suspect, you shouldn't be scanned. That's a fundamental principle of criminal law."**
>
> **Dr Elizabeth Farries, UCD Centre for Digital Policy**

The chilling effect

There's also a likelihood that (as we talked about with **bias and accuracy**) communities that distrust the police could be less comfortable with this tool. Policing Insight hasn't seen any England and Wales or UK-wide data on public support for LFR by ethnicity – an important factor for policing, given the lower levels of trust seen in some communities.

Andy George, President of the National Black Police Association, expressed his concerns about this: "Like other police powers and technology, we're worried about the detrimental impact on minority ethnic communities, particularly the Black community."

He continued: "I think we're setting up LFR to disproportionately impact the Black community in London at the minute. At any other time that would be bad enough. But with the crisis in confidence and the [current] feeling in the community, I think now's definitely the wrong time to deploy stuff into almost singular Black communities rather than other places."

In addition, the concern about a chilling effect – the idea that, even if someone's innocent, the presence of police LFR might make them uncomfortable or unwilling to visit that public space – is genuinely difficult to measure.

Professor Kyriakos Kotsoglou, Associate Professor at Northumbria Law School, told us: "FR has a chilling effect on anyone who might think: 'Oh, I don't want to be there in the public space when it's being used.' This isn't measurable, it's intangible…" But it could become a highly relevant factor in future legal cases, he explained. "The assumption that there will be this chilling effect is something that the courts don't have difficulty in accepting."

This chilling effect may grow as LFR gradually expands. For example, the use of LFR to manage public order issues – something we saw **Northamptonshire Police trial in 2023** at the Silverstone Grand Prix to deter environmental activists – creates a risk of discouraging people from engaging in peaceful protest.

Even if someone wasn't on a watchlist and wouldn't have been flagged up by LFR, a chilling effect comes down to people's own perceptions. If someone fears being scanned by that LFR camera for any reason, a deterrent can be created for innocent people just as much as it can for criminals in the area.

This issue becomes more complicated depending on how widely and how often LFR is used. For now, there are really only two forces regularly using it in England and Wales; and while more investment is on the way, Lindsey Chiswick told us that the Met currently "doesn't have loads of kit". In fact, it has just two LFR vehicles which also "double up as CCTV vans".

But imagine if, a decade from now, LFR is far more ubiquitous. It's become a fixture in the largest city centres across England and Wales on a daily basis, rather than a relatively rare occurrence.

Today, a commuter ardently opposed to FR could avoid Ealing Broadway station when the Met announces a one-off deployment. But in this 'expansion scenario', where LFR is used every day at this large station, it becomes almost impossible to do so. So at what point along this spectrum does LFR become unavoidable, a condition of being in our major public spaces?

It's this question that, as policing in England and Wales looks set to scale up LFR via **£4 million of new government funding**, will continue to be a running theme of the FR debate.

CLICK HERE
Article
Police remove 218,000 photos from facial recognition database
Dutch police clear up FR database
dutchnews.nl

CLICK HERE
Article
Britain is 'omni-surveillance' society, watchdog warns
Law 'is not keeping up with AI advances'
theguardian.com

CLICK HERE
Report
House of Lords report into FR
Conclusions and recommendations following a short investigation into the use of LFR England and Wales police forces
committees.parliament.uk

CLICK HERE
Report
The Future of Biometric Technology for Policing and Law Enforcement
Exploring the future of biometric technology for UK policing
cetas.turing.ac.uk

CLICK HERE
Article
Prime Minister launches retail crime crackdown
Assaulting a retail worker to be made a standalone criminal offence.
gov.uk

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Legal and regulatory uncertainty

There are remarkable global variations in the legal and regulatory frameworks governing facial recognition. An effective approach should balance the obvious risks against the potential benefits to secure the best possible outcomes for public safety.

All the complex considerations we've talked about in this chapter – operational value and bias, privacy and human control – should naturally inform how different jurisdictions manage the police use of facial recognition (FR) tools. An effective legal or regulatory framework should balance the obvious risks against the potential benefits to secure the best possible outcomes for public safety.

But across the countries we've explored, there are remarkable variations in the legal and regulatory frameworks that cover FR, and especially live facial recognition (LFR). This showcases the range of options available to governments trying to provide more certainty around the 'rules of the game' for FR use in policing.

For example, governments in Ireland and Sweden have both laid the groundwork for new legislation that would let the police expand FR under certain conditions. Across Europe, the EU AI Act has introduced a common framework for law enforcement use of FR, one that also requires individual states to pass their own laws before they can use it live.

By contrast, in the US and England and Wales, there's much less certainty. In the former, it was striking that more than one interviewee described a 'Wild West' approach to FR with little oversight or certainty. In England and Wales, there's a growing body of guidance about FR use, but there's still a complex mix of different legal powers in place rather than any single law.

Back to Bridges

This challenge is illustrated clearly by the long-running debate in England and Wales about whether the legal basis for the police use of FR is strong enough. This was most prominent during the Bridges case involving South Wales Police's FR deployments (covered **earlier in this report**). Ultimately, the Court of Appeal decided in 2020 that there were "fundamental deficiencies" in the legal basis that the police were using at the time.

In response, policing has taken several different actions. The College of Policing has created **authorised professional practice** (APP) setting out how forces should deploy LFR with appropriate safeguards. There has been independent evaluation of the police's FR algorithms via the **National Physical Laboratory (NPL) report**. And forces now publish their own legal mandate documentation, setting out the basis under which they deploy this tech.

But there are still significant limitations, despite these steps forward. It's widely accepted that the legal basis in England and Wales – in which no single piece of FR legislation exists – remains highly complex. As explained earlier in this report, policing personnel, activist groups and academics all acknowledge this reality.

Even the **Met's own LFR legal mandate document** (see next page) emphasises this complexity. As this multi-coloured diagram attempts to explain, the Equality Act, Data Protection Act, Human Rights Act, Regulation of Investigatory Powers Act, and the Protection of Freedoms Act all play a role in terms of relevant primary legislation.

Below that, there's oversight from four regulatory bodies and the Mayor's Office for Policing and Crime (MOPAC). Then there's a range of other important components ('levels 2, 3 and 4' below) that form part of this framework too.

While some may argue that forces in England and Wales should be more cautious and avoid using FR until a clearer legal basis is in place, the lack of a single legal framework is something that can ultimately only be resolved by politicians. The police are working with what they have, and that complexity is a challenge for them too.

The 0.6 question

Even though the College's guidance provides a lot of useful information, it has obvious weaknesses. It's produced by policing itself, so isn't a true substitute for an externally-developed and scrutinised set of legal rules. It isn't binding on forces, given that each retains operational independence – although it is true that the current scale-up approach, where South Wales Police teaches new forces to use LFR via mutual aid arrangements, makes it more likely we'll see common practice across the country.

A good example of its limitations comes with the 0.6 default threshold setting used in current police LFR algorithms in England and Wales. At that level, the NPL report found that police LFR systems avoid statistically significant bias in terms of race and gender.

> **"Not even in our local policy have we written that we'll never operate below 0.6. And I wouldn't do that because ... I could imagine if there was a suicide bomber on the run in London. And they'd gone to a station and we were able to get the LFR cameras out in the station… to try and find that one person."**
>
> **Lindsey Chiswick, Met Police Director of Intelligence, and NPCC Lead on Facial Recognition**

But Lindsey Chiswick, the Met's Director of Intelligence and NPCC Lead for FR, told us that there might be very narrow cases where policing would drop below that threshold. She said: "Not even in our local policy have we written that we'll never operate below 0.6. And I wouldn't do that because – and hopefully we'll never face

Continued overleaf ↘

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

the scenario where we have to – but I could imagine if there was a suicide bomber on the run in London. And they'd gone to a station and we were able to get the LFR cameras out in the station… to try and find that one person."

Such a scenario is thankfully rare, but it's not implausible. And it raises a significant point; it means the police *would* use LFR systems at a setting which is known to be racially biased.

In the context of an immediate and credible threat to many innocent lives, some false alerts in return for a higher chance of identification might be considered acceptable. It's a trade-off with obvious risks on both sides.

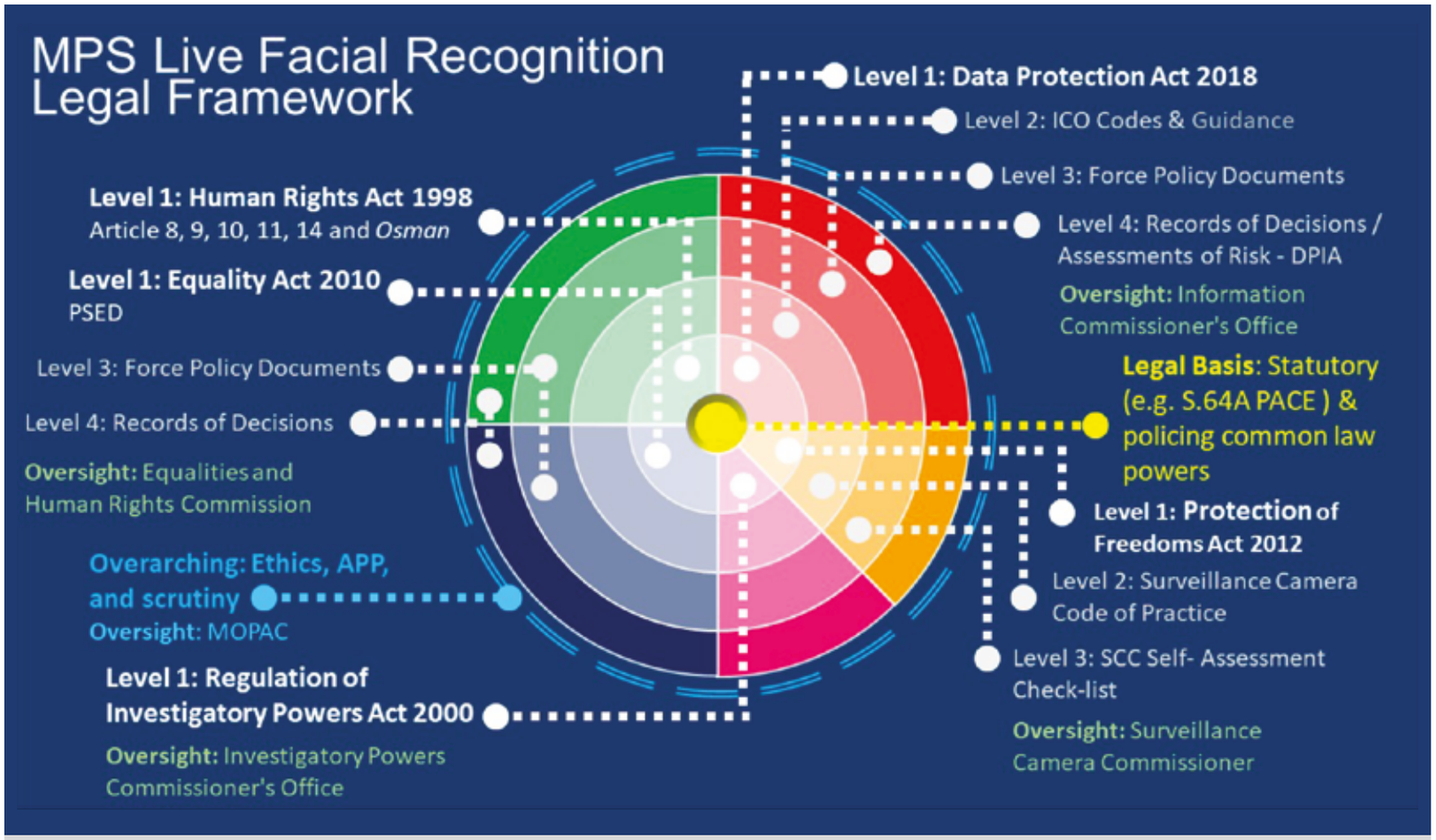
The difficulty is that the circumstances in which policing would use LFR in this way aren't listed in any legislation. They aren't in the College's APP, and they aren't something the public are likely to know about – at least until deployment data is published online after the event – and so could not realistically challenge.

Again, it's highly likely that, in a terrorist incident, the public might support this trade-off; but it highlights the inherent softness of guidance and a patchwork of legislation, rather than a fixed set of unified rules with more effective oversight.

The case for certainty

In January this year, the House of Lords Justice and Home Affairs Committee made a similar case. After a brief inquiry into the use of LFR by police forces, the Committee **wrote to the Home Secretary** and expressed their concerns.

They said: "We believe that, as well as a clear, and clearly understood, legal foundation, there should be a legislative framework, authorised by Parliament for the regulation of the deployment of LFR technology." They "question[ed] why there is such disparity between the approach of the UK and other democratic states in the regulation of LFR." And they suggested that the police and government responses to the Bridges case haven't done enough to give proper clarity.



Legal framework schematic key

- This is the legal basis for the action – ie the legal power(s) that supports the compilation of the watchlist and the use of LFR.
- This area reflects that biometric and other personal data is processed by the LFR system. It reflects the application of the Data Protection Act 2018 and underlying documents that govern and reflect this.
- This area reflects the relevance of human rights to the use of LFR. Some, like the right to privacy, will be engaged by those on the LFR watchlist and/or passing the LFR system. The engagement of other rights will be context dependant.
- This area reflects the relevance of equality considerations and the application of the Public Sector Equality Duty. It shows the underlying documents which also govern and show compliance with this duty.
- This area reflects the potential application of the Regulation of Investigatory Powers Act 2000 (RIPA). For an overt capability, it is important to have regard to RIPA to ensure the use of LFR does not become directed surveillance.
- This area reflects that LFR uses CCTV cameras to film those passing through the Zone of Recognition as part of the wider LFR system. It recognises the relevance of the Protection of Freedoms Act 2012 to CCTV in public spaces by policing in England and Wales.

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Much of this, by the way, aligns with the views of the public. According to research from the Alan Turing Institute, while only 5% of the public want biometrics systems that can identify criminals in crowded areas banned outright, 81% favour them being "explicitly regulated – such as through specific laws or provisions in laws."

In an exclusive interview with Policing Insight, Baroness Hamwee (who led the Committee during this inquiry) explained that "principled regulation" around police FR is crucial "because this is moving so fast… We can't be far off this spreading out region-wide, nationwide and then it becomes a very much bigger issue."

> **"I wonder whether, with what's happened over the Post Office, the public might be more aware of how things can go wrong and of the importance of regulation."**
>
> **Baroness Hamwee, Chair, Lords Justice and Home Affairs Committee**

She questioned whether recent events – such as the Post Office Horizon scandal in the UK, which led to innocent people being sacked and jailed for theft, based on data from a faulty computer system – may have bolstered the case for regulation too. "I wonder whether, with what's happened over the Post Office, the public might be more aware of how things can go wrong and of the importance of regulation," said Baroness Hamwee.

She also suggested that establishing a more fulsome legal framework would be better than relying on legal challenges to test it: "We're told on the one hand by the Met that there's a foundation in law, because it's the common law. But should an individual have to go through the expense and the huge strain of litigation just to test this? …It should not be left to an individual to instigate legal proceedings to explore whether what's being done is legal."

Is legislation likely?

The clearest example of a unified legal framework for FR is the EU AI Act. It establishes a set of rules governing AI systems (including real-time surveillance (or LFR) by law enforcement), offering a Europe-wide framework that's much easier to understand. And as Ella Jakubowska, the Head of Policy at the European Digital Rights (EDRi) Network told us, the Act requires states to create their own "national authorising law" before domestic police can deploy LFR tools legally.

By contrast, the US approach exemplifies the other extreme, with very little regulation or legal certainty at all. As Ira Reese, CTO of Global Security Innovative Strategies and a Member of the National Academies of Sciences, Engineering and Medicine's Committee on FR, put it: "At this point in time, FR in the United States is more or less equivalent to the Wild West." He added: "The laws and regulations have just not kept track with how powerful the technology is."

This uncertainty creates challenges for everyone who cares about FR, from the most ardently opposed to those who believe it can offer tremendous value.

For the police, a simpler legal framework is much easier to follow and comply with, leaving them less open to the kinds of legal challenge we saw in Bridges. For FR vendors, clear rules help them design their products to consistent standards and escape the uncertainty that every major business fears. For critical voices, knowing exactly what the law allows can aid efforts to challenge the police when they go wrong. And for the public, clarity opens the door to a more informed national debate about where, when and how this technology should be used.

In the absence of legislation, legal challenges often end up shaping the basis for use of FR. This comes with risks, as Professor Fraser Sampson – formerly the UK's Biometrics and Surveillance Camera Commissioner (now an academic and non-executive director at Facewatch) – told us: "We end up allowing litigation to write policy. Any lawyer will tell you that litigation is probably the most expensive, least predictable, and least flexible way of deriving policy. All it does actually – whether win, lose or draw – is undermine public confidence if they constantly see police chiefs being brought into court."

And yet, for policing, the challenge is simply that this is beyond their control. Politicians alone can grasp the nettle of providing legal clarity and, so far, there's been almost no sign that they're willing to do it.

At the time of writing, it's not clear what the current Labour Party policy on police FR is, and our requests for clarification also went unanswered. Given the polls suggest they're near-certain to form the next government, this is all the more concerning. In the absence of legislation, which can take many years to work through the political process, the police can only use what they have.

And it seems that legal challenges will be the likeliest route to change. With news that Big Brother Watch are sponsoring two separate **legal challenges to LFR use** by the Met and Facewatch, will we see a repeat of the Bridges case? It seems that courts, not legislators, will again be shaping the approach to FR – for better or for worse.

CLICK HERE
Policy
Live facial recognition
Guidance for the overt deployment of live facial recognition (LFR) technology
college.police.uk

CLICK HERE
Report
Facial recognition technology in law enforcement equitability study
Results of an evaluation of facial recognition technology
science.police.uk

CLICK HERE
Legal
Live Facial Recognition: Legal Mandate
An explanation of the varied sources of law that regulate LFR
met.police.uk

CLICK HERE
Report
House of Lords report into FR
Conclusions and recommendations following a short investigation into the use of LFR England and Wales police forces
committees.parliament.uk

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight



4

Conclusion

Conclusion

Use of FR for public safety purposes is, at once, increasingly common and somewhat over-hyped.

After interviewing 34 different experts – policing leads and politicians, legal experts and activists from across the world – it seems that the use of facial recognition (FR) for public safety purposes is, at once, increasingly common and somewhat over-hyped.

On the one hand, retrospective facial recognition (RFR) is now used by almost all countries we examined in some capacity. In places such as the US, Ireland, Sweden, Canada, and England and Wales, there are clearly efforts to expand FR, whether by trialling live facial recognition (LFR) or scaling up existing capabilities. Although currently paused, the UK Government was **reportedly** planning to publish a new FR policy statement in June, with serious implications for law enforcement. And the EU AI Act both regulates and opens the door to greater use of LFR across Europe.

And yet, the capabilities used by law enforcement are in some ways more modest than the public might suspect. In England and Wales, only around a quarter of forces are apparently exploring potential use of LFR at the moment. Just two forces actually use it regularly, and the largest of those (the Metropolitan Police) has only two LFR vehicles at its disposal. And this country is, depending on your perspective, a leader or an outlier on FR. In places such as New Zealand, Ireland and the Netherlands, appetite for LFR appears limited or non-existent.

In many ways, it's the private sector taking the lead. Remember that way back in January 2001, the 35th Super Bowl saw private sector use of LFR in Tampa, Florida. Today, many retailers and stadia across the globe are exploring or already deploying LFR capabilities. Whether that's due to growing criminal threats in these spaces, greater financial resources, or because private actors face less scrutiny than police forces monitoring public

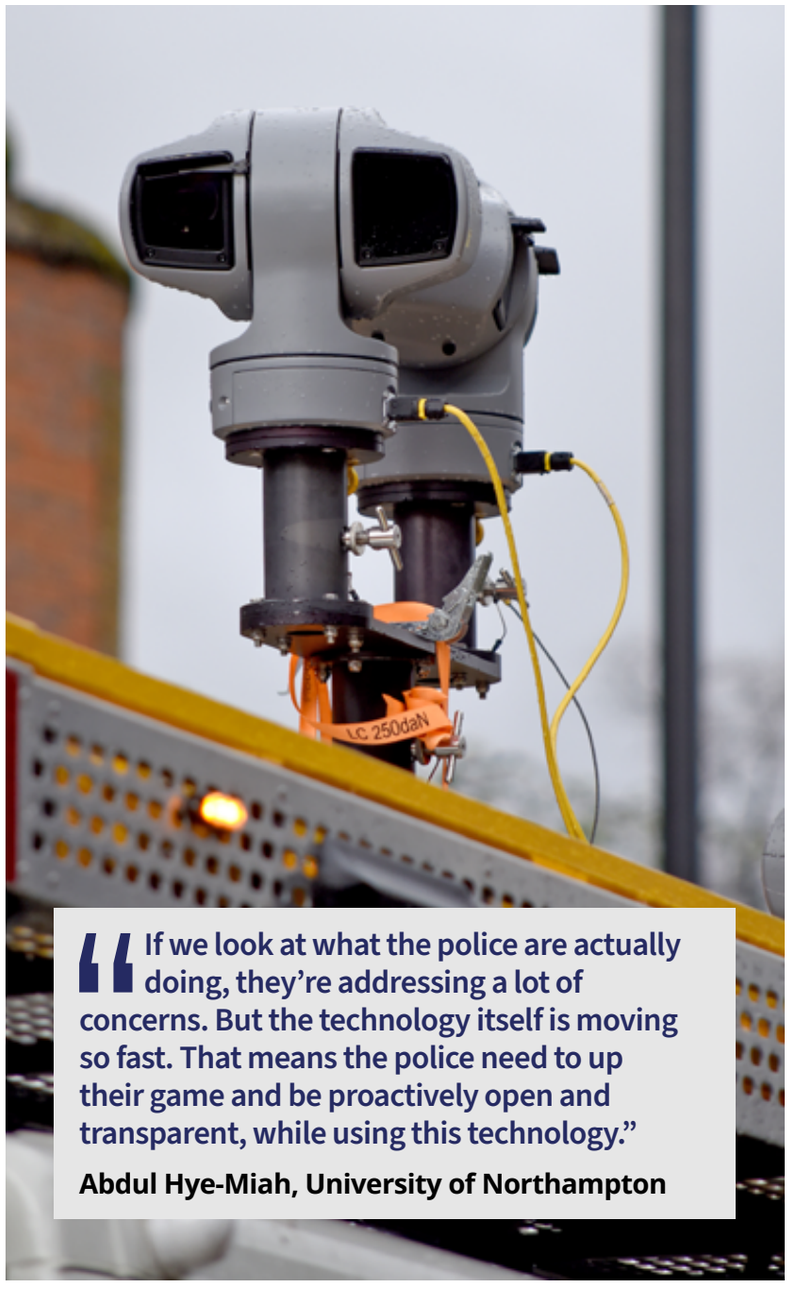
Continued overleaf ➘



> **"The capabilities used by law enforcement are in some ways more modest than the public might suspect. In England and Wales, only around a quarter of forces are apparently exploring potential use of LFR at the moment. Just two forces actually use it regularly, and the largest of those (the Metropolitan Police) has only two LFR vehicles at its disposal."**

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

Conclusion



> “If we look at what the police are actually doing, they’re addressing a lot of concerns. But the technology itself is moving so fast. That means the police need to up their game and be proactively open and transparent, while using this technology.”
>
> **Abdul Hye-Miah, University of Northampton**

areas, it’s a clear trend. It may even begin to normalise LFR before its use by law enforcement becomes commonplace.

But it does seem that we’re on the cusp of major change. Some interviewees drew comparisons between FR and the rise of generative AI – ChatGPT, DALL-E and the like – to show how quickly things can leap forward. FR isn’t really in that same category: there are higher barriers to entry and it can’t be scaled up user-to-user in the same way these tools have been.

Yet interest is growing. The EU AI Act may provide the first foundations for an expansion across the European bloc and, with relatively high public support in the UK, FR adoption in England and Wales may grow fast too.

However, policing should tread carefully. Throughout this report, we’ve seen a real division between technical questions and the more complex, intangible ones. It seems likely that many technical questions of bias and accuracy – the strict ‘effectiveness’ of an FR algorithm – can be more or less solved. Though that is also reliant on forces doing the less glamorous work of getting their facial image databases in order, a point we touched on in our previous report, ***From back office to business critical: Why information management should be a core policing function***. But the more challenging questions aren’t the technical issues that can be measured, fixed and ticked off as ‘solved’; they are more complex judgements that policing alone can’t make.

Is the deeper problem of FR bias about where and how policing deploys LFR systems, especially given different levels of trust across communities? How can we measure intrusion and chilling effects, even if innocent faces are always deleted? How do you ensure your human in the loop is an active agent, not a reassuring placeholder? And what is LFR’s strategic and tactical value, beyond identifying wanted people?

These challenges are even tougher to deal with because oversight just hasn’t kept pace. The EU has moved forward significantly here, but that’s in stark contrast with much of the Anglosphere. The US is the “Wild West”, according to two of our interviewees. There’s a lack of clarity about developments in Australia. And there’s a “patchwork” legal framework in England and Wales that’s been heavily criticised by a **parliamentary investigation**. Recent **legal challenges** supported by Big Brother Watch might have a seismic impact on police and private sector use in this jurisdiction too.

Policing itself ultimately cannot create legislation or regulation around FR. That’s the job of politicians and others outside of policing. But until political leaders grasp the nettle, it can play its part in leading a transparent national conversation with the public (and critical voices) about the risks and benefits of these tools.

As Abdul Hye-Miah, Senior Lecturer in Criminal Justice Studies at the University of Northampton, told us: “If we look at what the police are actually doing, they’re addressing a lot of concerns. But the technology itself is moving so fast. That means the police need to up their game and be proactively open and transparent, while using this technology.”

There’s a clear case – articulated effectively by some in policing – that FR can contribute to public safety. There are also major downsides, set out just as clearly by opponents.

In this report, we’ve tried to give you a fuller picture of this debate. The next step is for policing to help lead that important conversation. That means engaging the public, listening to their concerns, and building a genuinely trusted approach to the use of FR as a tool for public safety.

CLICK HERE

Report
From back office to business critical
Why information management should be a core policing function
policinginsight.com

Policinginsight

CLICK HERE

Report
The Future of Biometric Technology for Policing and Law Enforcement
Exploring the future of biometric technology for UK policing
committees.parliament.uk

HOUSE OF LORDS

Version 1.0 Copyright © 2024 CoPaCC Ltd/Policing Insight

A Policing Insight report

Find more thematic and research reports **here**

Interested in commissioning or sponsoring a future report?
Contact us to find out more: **enquiries@policinginsight.com**

CoPaCC
the police governance experts

Published by
Policinginsight

Copyright ©2024 CoPaCC/Policing Insight.