Senedd Cross-Party Group on Digital Rights and Democracy: Surveillance and Facial Recognition Tech, Minutes

28 June 2023, 10.00-12.00 PM, Online

Sarah Murphy MS – Chair

Open Rights Group – Secretariat

Panel:

Dominic Edgell – South Wales Police

Lee Jones – Chief Executive, Police & Crime Commissioner for South Wales

Madeleine Stone – Big Brother Watch

- Sarah Murphy MS – chair of the cross-party group – introduced the session, explaining that facial recognition is something she has been trying to get on the agenda of the Senedd for some time.

South Wales Police use of live facial recognition technology

- Chief Inspector Scott Lloyd from South Wales, attached to the National Police Chief's biometric function – a small team of people trying to help navigate biometric technology and how it's adopted in law enforcement – presented "the legitimacy of facial recognition technologies, as a capability in policing and law enforcement."
- He believes there is a role for facial recognition, which is a shared view of the majority of the public, he says, insisting the public's consent is important in their crime prevention and protection of the public.
- Therefore, they act in proportional, lawful and necessary ways – important for the debate to continue to ensure police are operating within the law.
- The criminal landscape is becoming more complex and sophisticated, so law enforcement has to innovate to respond to the complexity, particularly in the digital era where new and emerging frontlines of crime have been produced.
- The police officer will always make the decisions involved in law enforcement and technology should not fetter individual officers' discretion to make decisions in any given circumstances.
- There are three ways that the technology is deployed:

1. Restrospective facial recognition – the most tried and tested. An image has been obtained post-incident, which is then compared with other custody images that police may lawfully hold to try to identify the suspect so they can proceed with that investigation. That has been available since 2016.

2. Live facial recognition – the most contentious use of the technology. Live facial recognition cameras are used, supported by an intelligence case. The software receives the light feed and compares it against a watch list to look at individuals, after which point the image and the biometric template used for live facial recognition are immediately deleted.

3. Operator-initiated facial recognition – the newest form. Currently only used by several police forces and involves the tech on the officer's mobile phone and is used when the officer interacts with the public to identify who they are.

- Most police have used retrospective facial recognition locally since 2017. They would have access to a national and local gallery of images. It used to take about 10 days to identify individuals before any arrest could be made, so the necessary timeframe for the necessity test to be passed to access the images. With retrospective facial recognition, it can take 10 minutes. Almost 4000 matches have been achieved since 2017. Overall, it is quicker for individuals to be processed through the justice system with the tech.
- Lloyd gave a use case example of an individual who assaulted a woman on multiple buses in Cardiff and they were able to identify the attacker from the bus CCTV footage against 12-year-old custody images. With FRT it would have taken far longer to identify the individuals as it would have circulated among police officers and possibly the public to get a match.
- Moving to live facial recognition, South Wales Police are one of only a few forces currently deploying live facial recognition – it has been deployed on 70 occasions with 75 arrests resulting; there were no false arrests or complaints specifically concerning the technology save for two court cases.
- Operator-initiated facial recognition is the next iteration of the technology, where frontline officers will have it on their mobile phones. The rationale is that officers will be able to conduct a name check over their mobile devices. If an individual can't verify their details, they will use the tech, providing more options than taking DNA and taking them into custody. Lloyd says this is particularly pertinent if they encounter vulnerable persons, missing persons, people with mental health issues etc.
- Regarding people's rights, there are three primary use cases. Even though the technology has been broadly accepted by society as it is prevalent on mobile phones etc. However, it is right for law enforcement to be subject to the highest levels of scrutiny. There are two courts – the Divisional Court and the Court of Appeal. The court has instructed South Wales police to do more – look at who they put on the watchlist and where they deploy the technology and there needs to be a code of practice and amendments to local policies to remedy the issues found in the court.
- The surveillance camera code was amended in August 2021 and adopted elements of the judgement, as have Southwest police policy documents. The College of Policing, as a professional body for police, has also since published authorised professional practice for the overt use of live facial recognition.
- Also, while the court recognised there was no clear evidence that facial recognition was biased on the grounds of race or sex, South wales Police did everything it could to fulfil the public sector equality duty to understand any potential bias in the technology and there were three things they did:

1. They approached the National Institute of Science and Technology.

2. They sought clarity from some suppliers.

3. They commissioned the largest operational study of live facial recognition in the Western world, using the National Physical Laboratory, published earlier this year focusing on three protective characteristics – race, gender, and sex – across all three use cases.

- As the technology evolves, they recognise they may need to revisit their policies and the legal landscape.
- South Wales Police experience is the public is receptive to FRT when they explain how it is used. The Ada Lovelace Institute and the Information Commissioners Office also found strong public support for police use of FRT as long as it helps reduce crime.
- Lloyd said he was "absolutely convinced" of the benefit facial recognition technology has had in policing to assist in locating offenders.
- Questions were taken, including whether the current policies include children. Lloyd confirmed there are additional checks and balances concerning some protected characteristics, particularly focusing on children, because as you move through the age range, the technology's accuracy is affected.
- The National Physical Laboratory tests showed that for retrospective and operator-initiated facial recognition, there was no bias within the technology across race, gender and age. There are settings within live FRT where there is no bias across those characteristics either and South Wales Police will consistently operate at or above those threshold settings to ensure that there's no bias, he said. Also, there are checks and balances for the individuals on the watch list. He notes the potential of finding missing persons, particularly when an individual is juvenile.
- On thresholds, these may change if there is intelligence to support a search for someone specific. E.g. If a terror suspect is near a major event and you need to interact with them and search them to find out what they're doing there. There is a layered approach. The threshold will be the same across the board to ensure there is no bias but from a technical perspective, you can change settings based on watchlist categories or to find certain individuals. That will be evaluated according to the intelligence profile of the person on the watchlist and the reasons and risks concerned.
- The false positive rate is around one false alert per 60,000 people walking past a camera. No false positives were experienced at the recent Harry Styles and Beyonce concerts. There is also increased accuracy exponentially – according to NIST, the more accurate the technology, the less variation there is.
- The documents mentioned, such as the amended code of practice and Bridges appeal case (court judgment mentioned before), can be found online on the surveillance camera and biometrics commissioner's website. The College of Policing website will hold many policy documents – as will South Wales Police's website.
- There is a concern that the tech would be used for the right to protest as seen at the King's coronation but Lloyd said they had never deployed it and it is tricky and delicate – so when they deployed a, say, at the Harry Styles concert, they'd be looking for terrorism suspects and if a protest turned up they wouldn't be able to use it to police that. But he said you can never say never but the policy documents should dictate the right balance to be struck when making policing decisions of that sort.
- Decisions around which concerts the tech was deployed at (for instance, it wasn't deployed during the Cold Play concert) are made by the Assistant Chief Constable with scrutiny from the Police and Crime Commissioner. Intelligence is evaluated and decisions are made

amongst a “gold, silver and bronze structure,” the capabilities best suited to mitigate that risk.

The Police and Crime Commissioner’s role in overseeing facial recognition technology

- Lee Jones, Chief Executive of the Police and Crime Commissioner for South Wales, gave representations and an overview of the Commissioner’s role. One of the key roles is holding the Chief Constable in force to account for the delivery of an efficient and effective service stemming from the Social Responsibility Act but it is not to interfere with operational policing. I.e. they rationalise what resources are deployed but the Commissioner can provide oversight that the rationale is justified.
- There are formal and informal channels for that oversight and thorough governance arrangements, including formal scrutiny committees.
- The Commission also sets the priorities for local priorities policing through its Police and Crime Plan, which is available on the Commissioner’s website.
- Jones’ key responsibility is coordinating on the Commissioner’s behalf and facilitating public scrutiny of the role of holding the chief to account. Local development of facial recognition technology has been a primary concern and they have had oversight and provided information for the mentioned court cases. Their approach is guided by standard policy but they can take the public’s concerns and academic expertise into account – it has an independence perhaps people aren’t aware of.
- There is a Police and Crime panel that consists of members from each of the seven local authorities in the South Wales area and also independent members.
- They have seen progress in the tech and response to the court case; a demonstration will be given to panel members on how the tech will operate.
- They have a police accountability and legitimacy group – a group of independent members from among the community, race equality camps and young people’s organisations, etc. They bring in different perspectives around stop and search and facial recognition particularly.
- A scrutiny board with Jones and his team members proactively develops feedback using public engagement, experts, reports from academia, etc. Technological aspects are also all fed back up with the former in a report to a Commissioner strategic board, which is the most senior accountability board chaired by the Commissioner, holding the chief and his senior team to account as well if there’s a need for any escalations or discussions of key points, whether it be for example, a court case, or issues that are going to be escalated to Police and Crime panel.
- Jones said they are also cognisant of the ethical questions here. An ethics committee and experts have been involved from the beginning of the development of the tech.
- There have been changes introduced but it is an iterative process. They’ve identified issues around accuracy when identifying people of colour and younger people, but as the technology is used more, further issues will arise.
- The independent ethics committee is independently chaired, it has independent members that are appointed to sit on there with a variety of backgrounds from within the community.

- Each deployment is decided on individually based on the intelligence picture. The Harry Styles concert warranted live facial recognition, he says, because it was a younger demographic, it could draw in sex offenders and could be a terrorism target. It was also a concert where everyone wanted to be, so the potential to locate missing persons was high. Therefore, there is no carte blanche to using the technology. They identified 714 individuals – high priority, outstanding warrants, missing persons and potential terrorism suspects.
- While they can't get involved in operational policing, they do an annual survey, which returns feedback on policing styles.
- Regarding children, representatives from the Children's Commissioner's Office are members of the police and accountability group so that feedback can happen that way. There are generally good lines of communication between commissioners too.
- In answering a question about whether people are allowed to cover their faces, which happened during COVID a lot, the technology doesn't need to see the full face to work. They can hide their faces if they like and the use of live FR is advertised. It is a significant prevention tool as well as an identification mechanism.
- There are general powers the police have to tell people to remove their head coverings or face coverings etc, not specific to facial recognition. Also, if people walk past cameras with a 'bag over their head,' it may lead to a conversation.
- Jones and Lloyd reassured that there was community engagement in a continued way and a lot of work was going into explaining the technology and there is involvement from the community on the various panels. More engagement needs to happen in a targeted way.
- They take the issue around bias seriously and are working with the European Commission of Human Rights – they've started an investigation around AI and facial recognition technology and have published their three-year plan focusing on the use of policing use of AI.
- The frustration from the public is apparently that the police aren't using the technology far more broadly than they are.

Civil society concerns around live facial recognition technology

- Madeline Stone, the legal and policy officer at Big Brother Watch – a civil liberties and privacy campaign group based in the UK – also presented.
- Big Brother Watch has been following the South Wales Police, Met Police and private sector use of facial recognition technology and they attend deployments.
- Stone stressed that Big Brother Watch wasn't absolutist in their approach – finding individuals responsible for criminal wrongdoing differs from surveilling football fans at a match or protesters.
- They admit there may be a place for retrospective facial recognition within policing because it is far more targeted and proportionate. Although the concern is that there still need to be legal safeguards around how this is used and no legislation dedicated to it.
- Live facial recognition poses the most significant threat to human rights, privacy and civil liberties in the UK because it is untargeted and "mass surveillance," scanning everyone that

walks past it. “We believe that is a privacy-obliterating technology. There are serious issues with accuracy and discrimination. And lastly, this technology is enormously undemocratic.”

- Anyone’s biometric data can be scanned, which is enormously sensitive and is subject to significant protection and additional protections if processed. It’s compared against a watch list. This tool turns traditional policing on its head. Typically, surveillance is preceded by suspicions – an individual would be suspected with evidence that warrants surveillance or there’s a risk of them committing a crime or other reasons for investigation. Live facial recognition starts with the mass surveillance of everybody who walks past a camera and then compares them against a watch list.
- “It ultimately turns us into walking ID cards with our faces, being used as barcodes that can be scanned.”
- It’s a momentary scan and the data is deleted afterwards but it’s the equivalent of police officers demanding the fingerprints of everybody who walks past and to check their identity. And then deleting it afterwards. But the scan happens without necessarily your knowledge or consent.
- It so far has been deployed on top of vans, and deployment can last up to eight hours.
- It is being normalised and we will see it more widely used, said Stone, and eventually within CCTV networks. But we expect an amount of privacy and not to be monitored every moment, wherever there are cameras. Its use is akin to what is happening in China and Russia. This type of technology forms the backbone of a police state.
- There are minimal safeguards and the technology does not work perfectly, while millions have been invested, so it should be more accurate.
- Stone says other statistics suggest a higher number of alerts for fewer incidents and many more false positives – since 2017, 90% of all matches have been false positives,
- The technology is regulated by a patchwork of guidance and the Commissioner’s Code, which is not legally enforceable.
- There are no legally enforceable specific facial recognition guidelines that oversee how police use it and no law that mentions facial recognition specifically. So the guidance that police have, which the College of Policing has authored, means that who can be put on watch lists is broad-ranging.
- Some of the incidents that are recorded as true positives by the police are actually on people who should not be on watchlists, to begin with. For example, in London, a young man was flagged by facial recognition and was recorded as a true positive but he should never have been on the watch list as he had been released from prison a few days before and there was no intelligence case, he wasn’t wanted for any crime but put on a watch list. Even though he has done something wrong in the past, he has gone through the criminal justice system and paid his debt to society but is still stopped and ID’d by police and questioned, which can be stressful.
- The core baseline for using this type of technology is necessity and efficacy. The National Physical Laboratory independent study commissioned by South Wales and the Met looked at the accuracy and discrimination within the technology. The 1 in 60,000 false positive rate was cited based on the overly large watchlist and these watchlists are growing. As they

grow, the accuracy will weaken and there will be even more false positives. The report's assessment of bias also found that at certain thresholds, there is a difficulty matching accurately – in particular – young Black females.

- When so much trust needs to be nurtured in communities, this is not the time to invest so much money in deploying this type of technology.
- Beyond algorithms, one must note where the deployments take place and who it is targeting – and the first deployment was at Notting Hill Carnival, where London's Black British and African Caribbean communities come together, which speaks volumes about who the Met are targeting.
- It's also been used in predominantly Black areas of London and it's important that human rights groups observe these deployments. The people who are stopped and misidentified time and time again are young Black men and often in quite aggressive circumstances when they might not understand what is happening.
- There has never been a debate about facial recognition in the House of Commons. The only committee in Parliament to examine the use of live facial recognition called for an immediate stop to its use by the equality and human rights regulator.
- In democracies, there is a move towards stopping its use; for instance, US states and cities are increasingly banning this technology – New York City is currently considering a ban on this technology in public spaces. The European Parliament voted to ban facial recognition in its entirety without any loopholes for police use because of the recognition of the human rights threats to this technology. The UK is increasingly becoming an outlier in its approach to live facial recognition.
- To counter Stone's position, Lloyd said that they are seeing improvements in technology and that is why they want to use the technology. But he agrees there should be primary legislation.
- The point was made that until people, particularly Black communities, start trusting the police, they will not trust these technologies.
- Stone said there has been backlash from race equality groups and Essex University found human rights risks with the technology.
- She also said it's important to consider who is put on watchlists as it's not just sex offenders and terrorists; the categories of people who can be put on the watch lists, according to the College of Policing guidance, are "extraordinarily broad," and not limited to people suspected of criminal offences – witnesses and victims of crimes can be put on a watch list, and associates of any of these people can also. For example, at the anti-arms fair demonstration in Cardiff, live facial recognition was deployed and campaigners who were not wanted for any criminal offence were placed on watch lists purely for intelligence purposes. That formed the basis of the legal challenge to South Wales Police. (Ed Bridges, local councillor and anti-arms campaigner, was put on a watchlist while he was at a deployment). People with mental health issues have been put on watch lists in London. An NHS list of people with certain mental health conditions is also being placed on these watch lists. The picture is far broader than some of the hard-hitting case studies that the police are publicising.

- Jones said the information was useful. He'll ask further questions about the checks and balances locally.
- The point was made that South Wales Police's resumption of live facial recognition deployments is coinciding with a government refresh of its counterterrorism policy, particularly around preventing terrorism – obligations around venues, support of live FR around high profile concerts aligns with that; also profiling and referring people on to the Prevent database, which is itself subjected to an increased number of false positives. Open Rights Group is concerned about people ending up on different databases and watch lists and is curious about that pipeline potentially going on to these watch lists and the racialised aspect of that.
- In terms of the public buy-in, which kind of demographics does that come from as it would change according to age, ethnicity area. It matters where trust is being built.
- Murphy asked if data on individuals could be shared for different purposes between departments. Referring to an inquiry that the Equality and Social Justice Committee did, which was around migrant women who are victims of domestic violence, and how they would hear from the Home Office after reporting an incident to the police. There was also a case with the Manchester Metropolitan Police where people with visible disabilities at an anti-fracking demonstration were passed to the Department for Work and Pensions to threaten people's benefits because 'if they were well enough to go to a demonstration they could also work.' Therefore, what is the likelihood that facial recognition technology would facilitate that?
- Lloyd said that would be concerning and was not aware that was happening.