Wales Cross Party Group on Digital Rights and Democracy, 3 February 2023

Surveillance and Facial Recognition Tech

Speakers:
Sarah Murphy MS (Chair)
Ed Bridges (Ed Bridges vs South Wales Police)
Madeleine Stone (Big Brother Watch)
Stephanie Hare (Researcher)

Introductions

- Sarah Murphy MS's introductory remarks included an update on the inquiry through the lens of data justice. Now the Senedd is engaged with an expert advisor, which is very important to support this work.

- Chloe Rees, work with Murphy, also secured a debate on biometrics in schools this March, in the chamber. People are welcome to send things over to be included.

- Last June Murphy asked the minister questions on use of AI and the risks around the use of technology as well.

- The response was that those responsible for using or deploying algorithmic decision making tools must be required to understand the capabilities and limits of these tools, consider carefully whether individuals will be fairly treated by the decision making process and that there are appropriate levels of human involvement in the decision making process. They must put structures in place to gather data and monitor outcomes for fairness, understand their legal obligations, carry out risk assessments and document risk of bias.

- They also asked what assessment has the minister made on the impact of deployment of facial recognition by South Wales Police on the right to privacy? And what assessment the minister made of the discriminatory impact of facial recognition technology on women and ethnic minorities.

- The response was that use of live facial recognition is an operational decision for the police and policing is reserved matter and the responsibility of the Home Office.

Indiscriminate and disproportionate incursion of privacy

- the first speaker was Ed Bridges, a civil liberties campaigner who argued that the capturing of 1000s of faces by the Welsh force was indiscriminate and disproportionate in the world's first legal challenge to police use of this tech – a breach of rights to privacy, data protection laws and equality laws.
- In September 2019, the High Court decided that live facial recognition does interfere with the privacy rights of everyone scanned but the current legal framework provides sufficient safeguards.

- In August 2020, the Court of Appeal agreed with Liberty's submissions and found South Wales police use of facial recognition technology breaches privacy rights, data protection laws and equality laws.

- On two key counts, the court found that Bridges' right to privacy under Article 8 of the European Convention on Human Rights had been breached.

- On another it found that the force failed to properly investigate whether the software exhibited gender bias.

- Bridges first brought that challenge after the initial use of facial recognition technology in South Wales in 2017, taking until August 2020 for the Court of Appeal ruling.

- Bridges raised the challenge as a citizen and sees automated facial recognition's (AFR) creeping use within society as problematic.

- The main reasons for the contention is the lack of consent, the chilling effect of AFR and the system's inherent bias.

- On consent, important to note how the tech makes a biometric map of your face, and checks it against a database. That biometric map is something which is unique to individuals, more akin to a fingerprint than an image. Imagine if South Wales police or other force stopped people while they walked down their local high street and took their fingerprints on the off chance that they were a wanted criminal; people would object to that.

- Bridges explained he felt that way the first time his image was scanned by AFR, he felt his privacy had been invaded, even though he was acting perfectly legally.

- In the successful appeal the Information Commissioner said that AFR involves the collection of personal data on a "blanket and indiscriminate basis."

- Capturing people's data in that way without their consent means that we are all effectively being treated as criminals, a principle to which most reasonable people would and should object.

- Regarding the chilling effect. Bridges notes that his second experience of AFR was when it was deployed by South Wales Police at an arms fair in Cardiff where he was protesting with Quakers and peace groups. AFR was deployed that day and has been deployed to other peaceful protests since in a way that makes people feel that they are being criminalised, or at the very least having their their image and data captured by the police for exercising their lawful right to peaceful protests. That has a chilling effect – how can people peacefully protest against the state, when the state is scanning them and capturing their personal data? Should the same thing happen in China or Russia, it would be labelled an abuse of power.

- On bias, AFR can only ever be as good as the algorithm which supports it. There's plenty of data, which shows the facial recognition software is less effective when it comes to successfully recognising female faces and non white faces. In Bridges' case, the Court of Appeal noted that South Wales police, "never sought to satisfy themselves either directly or by way of independent verification, that the software programme in this case, does not have an unacceptable bias on grounds of race or sex."

- There has never been a full public debate or even a public consultation about the use of AFR in South Wales. He posed: Why is that? Why is this technology being imposed without any attempt to understand public concerns, or to engage in a meaningful way with the legitimate questions of civil liberties, campaigners and organisations? Is that something that we think is right and is that how we think the state should be operating?

Incompatible with democracy

- Madeleine Stone from Big Brother Watch (BBW), specialise in surveillance technology and its impact on human rights, spoke of the organisation's experience tracking the growth of facial recognition in the UK from its first use case.

- Facial recognition was first announced as a trial in 2016 and BBW has been attending deployments of facial recognition in London and in Cardiff since 2017. They have been to all London deployments.

- Describing what it is like for people on the ground, she says it feels like masses of police officers circling you and with this huge van scanning your face.

- There are private company uses of facial recognition now such as by the Southern Co Op, which uses live facial recognition in 35 of its stores across the south of England with even less oversight than police forces.

- Live facial recognition is the most chilling use of facial recognition in the UK, according to Stone, and the biggest risk to privacy.

- BBW is not absolutist about surveillance, there is a place for targeted proportionate surveillance of those who are suspected of wrongdoing; nor entirely against the use of facial recognition by police forces. Some uses, they say, for example, retrospective facial recognition, they accept might have a place in policing, with extremely strict safeguards, which currently don't exist either.

- Live facial recognition essentially carries out ID checks of every passerby, it doesn't distinguish between innocent and guilty people, and ultimately treats everyone like suspects in a police lineup.

- Ina dystopian world, people often cite microchips under the skin, but when the police can scan your face, they already have a barcode they ca check against a database, so they don't need microchips.

- Facial recognition is being used in one off deployments by police forces in the UK as well as China and Russia. These same countries aren't particularly known for respecting human rights. In Iran right now, facial recognition is being used to spot women who are not wearing burkas. It is not a kind of technology that sits comfortably within a democratic rights respecting country, said Stone.

- Facial Recognition changes our relationship with the police – we are policed by consent and have a strong history of rejecting ID cards; police aren't allowed to demand ID for no reason – FR scans everyone, however.

- Facial recognition is thus appalling for privacy and our right to anonymity in public spaces.

- Discrimination and bias are also byproducts, beyond algorithmic bias to misidentification and changes the way that police treat certain people. A

- Police are often treat people quite disrespectfully when they're stopping them, even if there's been a false match, and they can be aggressive.

- For example, at a deployment in Romford in London, a 14 year old young black teenager in school uniform, came home from school and was misidentified by facial recognition. As it was his first experience, he didn't know what was happening when he found himself surrounded by plainclothes officers and they called him into an alleyway, asking for his fingerprints and his ID. He didn't know they were police officers, before uniformed officers came up. He didn't have ID because he was a

14 year old and tried to use his school tie to show which school he'd come from to verify his identity. The experience shook him.

- “That is a really negative experience to have with police at such a young age. And it leaves him not only with the idea that the police might be racist, but also that technology might be racist. And that's something that is a lot more difficult to fight back against, if you feel like the various systems that polices are using have biases against you.”

- Even if this technology did work perfectly, the problem is that a lot of the people who have been loaded onto these watch lists are disproportionately from ethnic minorities, which means that routinely, people from ethnic minorities are being stopped and misidentified – something BBW has seen in London on multiple occasions.

- In another example, a young black teenager in Oxford Circus was shopping with his friends and was surrounded by several police officers. He wasn't allowed to go until he gave his fingerprints or showed his ID. He was held for 15 minutes because the police officers were eager to find something on him. Eventually had to let him go.

- These deployments are one offs right now but as this technology gets more investment, it will be far more regular. If we amplify the amount of stops that we've seen, on a bigger level, we could have, you know, a considerable number of people being wrongly identified.

- It can be scary, the Territorial Support Group have also been present, and they have tasers with them.

- The risk with this kind of technology is a slippery slope and how far it can go.

- It is also not a particularly financially viable way to continue to use facial recognition, if police forces want to be using it constantly. It begs the question, could we see public facial recognition being used in CCTV? That has been suggested in Ireland and what has been happening in China and Russia. And that seems like that would be the natural endpoints, this kind of technology, which would make it extremely pervasive and pose a real risk to rights.

- Given the current trust and the crisis of trust in police forces right now, should police sources be using such a controversial and invasive technology, when there has been no real democratic oversight, asked Stone.

- She says the lack of democratic oversight for this technology is staggering.

- There are a litany of human rights risks of technology to privacy, to freedom of expression, in the context of protests, the risks of discrimination to women, people from ethnic minorities and people with mental health problems – it has been used to prevent people with mental health problems entering certain events, so people who are not suspected of any crime.

- It has never been debated in Parliament.There is no law that contains the word facial recognition. There is no legislation that that oversees how it is used. The only parliamentary committees that have looked at it have recommended a moratorium on its use, which was ignored.
- “Police forces are really writing their own rules on how this technology is being used, which is pretty staggering.”

- It is a highly controversial and political decision to deploy and Stone say it’s not appropriate for police forces to be making the decisions on its usage.

- Police forces have been quite reluctant to give full transparency and it's taken several years of organisations like BBW and Liberty pushing and slicing under legal challenge to get full transparency policies used.

- The Met Police commissioned a review into how live facial recognition complies with the law and human rights risks, which said it posed a serious threat to human rights and the review was buried.

- While stone said Murphy had been doing great work raising awareness in Wales, the Welsh Parliament needed to be more involved as it has a massive impact on Welsh citizens. There needs to be far more democratic accountability and scrutiny of how this works.

- Stone finished with a comment from one French exchange student misidentified in London at deployment last year who was stopped by facial recognition, surrounded by officers had his fingerprint taken and held for about 15 minutes. When BBW spoke to him afterwards he said, I knew that you had this kind of technology in China. That's something to reflect on about the kind of path we're going as we just kind of rely on these invasive technologies more and more.

Children can't consent

- Stephanie Hare provided a presentation and explained how she wrote a book, called, Technology is Not Neutral: A short guide to technology ethics," with an entire chapter on facial recognition.

- Hare reflected on the evolving attitudes towards ID and biometrics. Boris Johnson for instance once said he'd eat the ID card if you asked to see it, but under his government, had actively promoted biometric and surveillance technologies.

- Some forms of technology and processing of data are well tested, going through border checks, for instance, unlocking your own smartphone but many use cases are up for debate, including identifying someone in a crowded room, which is what we're talking about, as well as anything to do with children.

- There is an update due from the Biometrics and Surveillance Camera Commissioner's office in February with the annual report will be laid in Parliament. They can be asked for a briefing note on it.

- As civil rights differ with the devolved administrations it is important to note that Police Scotland does not use FR. In 2020 they confirmed that they had no plans to use it at the time. What's happening in Northern Ireland and Wales may differ to England.

- It's hard to find algorithms free form bias, and it's the data as well and the people making the technology and the composition of their teams. Bias gets baked in at every stage.

- Misuses and bias related to technology becomes known by people so the police should be aware that it causes a trust issue if they are using it and communities of colour don't trust their use of it.

- Britain made worldwide headlines last year because of facial verification technology, which is a form of facial recognition being used in schools in North Yorkshire.

- When Hare asked the Scottish biometrics commissioner about this they said it was not their remit as it didn't involve crime but they thought that children in school in Scotland should be able to sit in class or take school meals without being watched
and recorded. That feeds into the rules around proportionality and necessity.

- The ICO have just declared that the technology was deployed in a manner that was likely to have infringed data protection law and that it was unlikely compliant with GDPR.

- It is important to ask whether children can consent. Can they read all the research and the legislation to make an informed choice? They will liekly comply to get on with their day so the power imbalance is apparent.

- While children in Scotland are not covered by the Protection of Freedoms Act, Welsh children are. There is a questiona round conditioning young children to be surveilled in this way, and teaching them to use their bodies effectively, to transact to borrow a book from the library, pay for a school lunch in the canteen, or even take registration.

-In HAre's view the technology should not be used at all on kids and a special protection should be in place.

- There has been little parliamentary effort in getting oversight.

Further action

- some groups were name checked as doing good work monitoring the development of policies and technologies related to facial recognition. E.g BBW, Liberty, Open rights group, Algorithmic Justice League, the Runnymede Trust, the Racial Equality Network and the Joint Council for the Welfare of Immigrants.

- Writing to your elected representative is incredibly important as well. The more emails they get from their constituents the more it starts to enter their consciousness.

- As policing and justice is not devolved in Wales, although discussions are happening around that, there is little that can happen in the Senedd to challenge AFR.

- Data protection legislation provides you with some rights – for instance, if you are at a football match and the police are filming a section of the crowd that you're in, you do have rights under data protection legislation to write to the police force and ask for footage of a crowd that you might be part of and they have to provide you with that but there is no equivalent around the use of of AFR. It is the Wild West in legal terms.

- A lot of CCTV cameras now have extremely advanced capacities, like facial recognition and motion analysis, gender recognition, gait analysis, crowd analysis, object detection, mask recognition, temperature recognition. BBW found a Chinese state owned camera company Hikvision, which is linked to serious human rights abuses in China.

- They were also advertising ethnicity recognition in the UK, the same technology that is used to monitor, detain and persecute Uighur Muslims in China. That shows how out of control surveillance has become in the UK in terms of CCTV.

- It's impossible for the ICO to keep track of every CCTV camera.

- Further links for information:
https://londonpublishingpartnership.co.uk/technology-is-not-neutral/
www.harebrain.co
https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/
https://www.netflix.com/gb/title/81328723
https://www.huntonprivacyblog.com/2020/08/12/uk-court-of-appeal-finds-automated-facial-recognition-technology-unlawful-in-bridges-v-south-wales-police/
https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/
https://docs.google.com/document/d/e/2PACX-1vSX_oBK2O-lseme88chci-3iXFXmUY_v3OC90r4b4Ri-FBptN6Y1O0KY7nyjARCS_hjnhwrr1BjKVHq/pub
https://scotland.openrightsgroup.org/