OFFICIAL REPORT
AITHISG OIFIGEIL

Justice Sub-Committee on Policing

Thursday 5 December 2019

Session 5

The Scottish Parliament
Pàrlamaid na h-Alba

Thursday 5 December 2019

CONTENTS

JUSTICE SUB-COMMITTEE ON POLICING
11th Meeting 2019, Session 5

CONVENER

*John Finnie (Highlands and Islands) (Green)

DEPUTY CONVENER

*Margaret Mitchell (Central Scotland) (Con)

COMMITTEE MEMBERS

*Jenny Gilruth (Mid Fife and Glenrothes) (SNP)
*James Kelly (Glasgow) (Lab)
*Fulton MacGregor (Coatbridge and Chryston) (SNP)
*Rona Mackay (Strathkelvin and Bearsden) (SNP)
*Liam McArthur (Orkney Islands) (LD)

*attended

THE FOLLOWING ALSO PARTICIPATED:

Griff Ferris (Big Brother Watch)
Dr Ken Macdonald (Information Commissioner's Office)
Tatora Mukushi (Scottish Human Rights Commission)
Matthew Rice (Open Rights Group)

LOCATION

Committee Room 6

Scottish Parliament

Justice Sub-Committee on Policing

Thursday 5 December 2019

[The Convener opened the meeting at 13:00]

Decision on Taking Business in Private

The Convener (John Finnie): Feasgar math, a h-uile duine, agus fàilte. Good afternoon, everyone, and welcome to the 11th meeting in 2019 of the Justice Sub-Committee on Policing. We have not received any apologies.

Before we start, I would like to make some brief comments about the resignation of Susan Deacon as chair of the Scottish Police Authority. I am sure that all members will want to thank her for her service and wish her well in future endeavours. We note her comments on the governance and scrutiny of policing, which will be issues for the Justice Committee and the Justice Sub-Committee on Policing. I am sure that we will return to those issues in the new year and consider what further work, if any, is required.

Under agenda item 1, the committee is invited to decide whether to take in private items 4 and 5, which are consideration of evidence that we will hear under item 2 and consideration of our work programme. Is that agreed?

Members *indicated agreement.*

Facial Recognition Technology

13:01

The Convener: Under agenda item 2, we continue our inquiry into how policing in Scotland makes use of facial recognition technology. I refer members to paper 1, which is a note by the clerk; paper 2, which is a private paper; and paper 3, which is a written submission by Dr Diana Miranda of Northumbria University.

I welcome the witnesses. Dr Ken Macdonald is head of ICO regions at the Information Commissioner's Office, Griff Ferris is legal and policy officer at Big Brother Watch, Matthew Rice is Scotland director at the Open Rights Group, and Tatora Mukushi is a legal officer at the Scottish Human Rights Commission. You are all very welcome, and I thank you for your written submissions, which have, as ever, been very helpful to the committee.

We will move straight to questions. First, concerns are expressed in the submissions about the lack of an explicit legal basis for taking and retaining police custody images by Police Scotland. Would the witnesses like to comment on that?

Matthew Rice (Open Rights Group): The Open Rights Group has been concerned about that situation for a few years. It was brought to our and the public's attention via the independent advisory group on the use of biometric data in Scotland. As part of its recommendations, it suggested the creation of a Scottish biometrics commissioner. Alongside that, it pointed out that the Criminal Procedure (Scotland) Act 1995 makes no explicit reference to photography or the taking of facial images. There are descriptions of other types of materials that can be removed from an individual, but the specific issue of facial images is not captured.

In addition, the legacy systems that Police Scotland inherited have meant that some images that were captured were retained for longer than, say, DNA or other biometric material. That is an additional consideration, which is aligned with the fact that there was, in the first place, no clear statutory or legal underpinning for collection of the images. That has led to divergence between practice on DNA—retention and deletion periods for which are quite clear—and practice in the situation with custody images that we are in.

Dr Ken Macdonald (Information Commissioner's Office): We understand the concerns that Matthew Rice has expressed. We also understand that there are major issues with legacy systems that were designed a long time ago, and were not built as systems are now

required by law to be built—under the general data protection regulation and the Data Protection Act 2018—whereby privacy by design must be built in. Under the previous legislation, there was an implicit requirement to take such matters into consideration; under the new legislation, there is an explicit requirement to do so.

We know that the police authorities are looking at ways in which to handle such images more appropriately. As far as the legacy systems are concerned, we need to take the pragmatic view that wholesale deletion is not necessarily in the public's best interests, although we are obviously aware that there are risks to the rights and freedoms of individuals who have not been found guilty but whose images, unfortunately, are retained because of technical issues.

We certainly think that legislative measures that clarify retention and disposal periods will always be welcome.

The Convener: Is there something between wholesale deletion and deletion only of images that might be perceived to be not legitimately held, or that do not have a legal basis for their retention?

Dr Macdonald: I think that the problem is that the legacy systems were set up in a way that means that deletion is proving to be problematic, hence it is deletion either of all or of none, although I would have to check that.

Griff Ferris (Big Brother Watch): Matthew Rice has summed up the legal position very well. I would add that the position in England and Wales is very similar, and that there is an overlap between Police Scotland and police forces in England and Wales, in that they upload images to the police national database. Police Scotland has estimated that it holds about 1 million images on its databases. Police forces across the UK, including England and Wales, hold a total of about 21 million images. Those are huge figures.

For what it is worth, I would point out that England and Wales are in the same position in respect of having a system that is incapable of deleting images of unconvicted individuals either after their status has been finalised as not convicted, or they were not even charged, following arrest. The Home Office has said that, due to technical issues, it cannot implement deletion of the legacy images, although it is, we understand, currently reviewing all the images that it holds in order to decide whether it can delete them.

Tatora Mukushi (Scottish Human Rights Commission): From a human rights perspective, the proportionality of using such large databases of unconvicted or untried individuals is problematic. It certainly engages article 8 of the European convention on human rights. We appreciate the practical and technical difficulties that are involved in sorting out the databases, but in cases of current justice, it will become an article 6 issue if the presumption against retention comes into play and the police are still relying on databases that are full of images that should have been deleted. It is unfortunate that the systems were not designed in a more forward-thinking way, with privacy in mind. Looking forward, the police will face a stark choice: they might simply have to forego using what they have, and start again in a way that is human-rights compliant, because the impact of using unreliable systems would be quite severe and disproportionate.

The Convener: Thank you. I am not remotely technically minded. Is anyone on the panel in a position to say whether the images can be utilised, scanned or searched, notwithstanding that they are inappropriately or illegally held?

Matthew Rice: Ultimately, as I understand it, that depends very much on the quality of the images. Some of the technologies that we will discuss as we move further into the meeting require a level of fidelity and resolution to allow images to be read. The answer is not necessarily clear.

The Convener: For the avoidance of doubt, I meant custody images.

Matthew Rice: Exactly. I am not sure that the resolution of custody images is such that we could say that they could be added to technologies or datasets such as we might discuss later. Such use would depend on the resolution and quality of the image. As I understand it, some of them would be good enough—a custody image of an individual that has been taken during booking or arrest could be of such quality that it could be utilised. Police Scotland can answer on whether the images are good enough to be used in the new systems.

The Convener: On live facial recognition, one could take the view that introducing a new system when we have been unable to resolve existing problems with the previous system is foolhardy. Does anyone on the panel have a view on that?

Griff Ferris: Yes. One of our major concerns has been that police in England and Wales have implemented live facial recognition technology that utilises custody images from a database in which there are known to be hundreds of thousands of images of innocent and unconvicted people.

In 2012, in a judgment in a legal case in the English and Welsh courts, it was held that indefinite retention of custody images of unconvicted individuals is unlawful. To date, the images have not been removed, so it can be argued that the Home Office has not complied with the judgment. There have been a number of

reviews—one is on-going—but the requisite action has not been taken. Ultimately, unconvicted individuals' images are still held in the database—there are 21 million images in the database, and 12 million of those have been made searchable by facial recognition technology.

The Convener: Mr Mukushi referred to articles 6 and 8 of the ECHR. If use was made of any of the images that are illegally held or for which there is no legal basis for their retention, could that use be the subject of legal challenge?

Tatora Mukushi: I should explain that article 6 gives the right to a fair trial and the right to due process. If it was known that the police had used faulty or unlawfully held images in identifying suspects, or in any part of an investigation, that investigation would then be suspect. Forgive me—I do not practise criminal law on this side of the border. However, as far as I am aware, in Scotland a fairness-balancing exercise is done, first by the Crown Office and Procurator Fiscal Service in deciding whether to bring charges, and then by the court in determining whether evidence has been contaminated by such an act. If it was found that an image had been used that should not have been in the database in the first place, there would be arguments around that, so its use could certainly be subject to possibly successful challenge. The police should bear that in mind.

Griff Ferris: The Biometrics Commissioner in England and Wales has said publicly that he does not believe that such use would stand up to legal challenge.

The Convener: The witnesses will be aware of the recent court case in Wales in which an application for judicial review over use of live facial recognition was refused, and it was ruled that the technology is lawful. Do the witnesses have any concern about that judgment with regard to human rights and data protection? As I alluded to in a question to Mr Mukushi, is there any expectation that, if the technology were deployed in Scotland, there would be challenges on human rights and data protection fronts?

Dr Macdonald: As the committee is aware, the Information Commissioner's Office has issued the commissioner's opinion on use of live facial recognition technology, subsequent to the case of R (on the application of Bridges) v Chief Constable of South Wales Police. In that case, the court found that use of the technology had been lawful, bearing in mind all the other restrictions that are in place, including data protection legislation. Our view is that that judgment was on a specific case and cannot be applied as a general framework. The fact that that opinion on it is the first one that the commissioner has written emphasises the importance that she gives to the issue. Under the GDPR, she has a new power to produce opinions, which came into effect last year: that is the first one, so you can see that the issue is a high priority for her.

The commissioner's view is that we should look at each use of the technology individually, that a clear case has to be made for its use, and that that has to be recorded, as is required by the appropriate use policy under the Data Protection Act 2018. Every case should be looked at separately and a DPIA—data protection impact assessment—should be carried out. Use should be focused and narrowed down; the arguments for each use of the technology must be clear and understandable and made clear to the public, as use continues.

The judgment exists and we have to build on it. As is implied in the Information Commissioner's opinion and her references to the Surveillance Camera Commissioner, who obviously does not have jurisdiction in Scotland, anything that can clarify how we in Scotland would like the technology to be deployed would be helpful.

13:15

Griff Ferris: There are a number of serious concerns about the technology. Obviously, there is a challenge against South Wales Police; we have also brought a challenge against the Metropolitan Police and the Home Secretary on similar grounds. The case is currently stayed, but we hope to proceed as soon as the Metropolitan Police decides whether to roll out the technology on an operational and full-time basis. If Police Scotland were to implement the technology, it is very likely that that would be the subject of a human rights legal challenge. As has been mentioned, it is a very serious threat to the right to privacy and the right to freedom of expression and association, and there are serious concerns about its discriminatory use, notwithstanding its general complete ineffectiveness as a technology.

Matthew Rice: I reiterate what Ken Macdonald pointed out. The Bridges judgment was quite narrowly based on the facts that were available, and each of the deployments was scrutinised. It did not say, "This is a green light for facial recognition technology on a large or general scale."

I also echo Griff Ferris's point that the scope of intrusion that facial recognition would involve would make a challenge likely in Scotland.

Tatora Mukushi: I point to the conversation about a Scottish biometrics commissioner. There has been wholesale consultation of experts and the public, and there is pretty universal agreement that a code of practice should be in place for dealing with biometric data, and that that should probably be a precursor to introduction of the

relevant technologies. The independent advisory group that produced the draft code of practice pointed to facial recognition as being uniquely problematic because of its lack of efficacy and the lack of evidence of its usefulness. To proceed to roll out the technology without something that the Scottish Government, the Cabinet Secretary for Justice and Police Scotland have signalled that they would welcome, and without bearing those things in mind, would be extremely problematic.

Dr Macdonald: On processing, there are two options for the police in respect of deciding whether to operate the technology. One option is to base it on consent. That is an option in the sense that it is in the law, but it is a totally impractical condition for processing when a person goes out into public space.

The other option is to base the decision on the technology being strictly necessary for the police's purposes. That is a very high bar. It would have to be clearly demonstrated why using facial recognition technology was appropriate when it was being deployed, and why other policing methods could not be employed to get the same result.

The Convener: Thank you. That is very helpful.

Liam McArthur (Orkney Islands) (LD): Good afternoon. That is indeed very helpful.

I want to touch on the issues of necessity and proportionality. What are your views on the extent to which those principles have been considered in the trialling of the technology to date and the balancing of the cost to individual liberty and the proposed benefits to public safety, which is what we are really talking about? I take it that, given the legal challenges, Mr Ferris is not at all convinced. Will you go into that in more detail?

Griff Ferris: From the start of our investigations into the use of the technology—as early as the beginning of last year, when we tried to uncover how it was being used, often using freedom of information requests—our legal analysis and independent legal analysis from our counsel suggested very much that the way that the technology was being used was not necessary or proportionate under an analysis of article 8 of the ECHR, which is on the right to privacy, and the right to freedom of expression. We have seen it being used against people who have not committed any crimes at all and people who were merely on watch lists because they had mental health problems, and we have seen it being used at a political protest. Obviously, that engages very serious concerns around the chilling effect in relation to people's ability to demonstrate political views or beliefs.

Due attention has not been paid to the high bar that is needed when it comes to necessity and proportionality. Facial recognition technology has not been used just to target serious or violent crime. There has been the indiscriminate scanning of hundreds of thousands of people—I think that it was stated as part of the case in south Wales that an estimated 500,000 people had been scanned, whereas only around 30 or so arrests were made, with deployment taking place around 50 times. Given those numbers, we need to ask whether the number of people who have been scanned by the technology and had their biometrics taken, which is akin to the taking of fingerprints or DNA—that is the scale of the privacy intrusion that we are talking about with facial recognition technology—is proportionate. Is the making of that small number of arrests proportionate to the level of intrusion?

Liam McArthur: Like the convener, I am no technical expert on such matters. Does the way in which the technology operates mean that the already high bar of necessity or proportionality is unlikely ever to be met, given that, in capturing images of people, it goes well beyond those who might be the target of the process?

Griff Ferris: It is very much our view that, because of the indiscriminate nature of the technology—it scans everybody within view—it captures their image without their consent and potentially without their knowledge. On that basis, it is not and could not ever be compatible with human rights. The technology that police in the UK use can scan around 300 faces a second. That is the level at which it operates. Ultimately, that is the level of mass surveillance in a public place that it can carry out. For those reasons alone, let alone the chilling effect on freedom of expression, the discriminatory effect and its lack of effectiveness, we think that it should never be used in this country.

Matthew Rice: Within the live facial recognition context, there is a famous BBC video of one of the Metropolitan Police trials that Big Brother Watch attended that addresses the issue of proportionality and whether a person can opt out of being involved in the use of facial recognition technology. An individual was given a heads-up that the technology was being trialled down the street. He then tried to obscure his face as he walked down the street because he did not want to be scanned, which led to him being detained and questioned. There were subsequently some issues around that.

That highlights the question of the proportionality of the use of the technology. If an individual wanted to walk down the street and did not want to participate in its use, how could its use be balanced with their right to individual liberty? That video provides a stark illustration of the fact that the use of live facial recognition is not an opt-out system.

Dr Macdonald: I want to stress again that we have a higher bar than just necessity; the use of the technology has to be "strictly necessary". That is a much harder test to meet.

Throughout the Information Commissioner's opinion on the use by law enforcement of live facial recognition technology in public places, the need for proportionality is stressed, as well as the need to have a strong legal framework within which to work. That would help to guide the authorities towards using it only when the level of necessity was appropriate. It is a question of narrowing down the focus and using the intelligence that the police have to narrow the location in which the technology is employed and to reduce the volume of individuals who are scanned at any time. Rather than being used for wholesale 24/7 surveillance, it must be deployed only for very short periods. Every time its use is implemented, a data protection impact assessment should be carried out, as part of which the human rights aspects should be considered.

Liam McArthur: You have talked about the massive extent of the capturing of images that the use of live facial recognition technology results in. Earlier, Dr Macdonald talked about the impracticalities of ever gaining meaningful consent. I understand that Mr Ferris has taken a view that the downsides are insurmountable, so deployment is wholly impractical. Who should be tasked with ensuring strict necessity or proportionality? I assume the view is that it cannot simply be left to Police Scotland or individual police forces, so who can make that decision?

Dr Macdonald: It is up to yourselves as members of the legislature to determine exactly what framework can be used.

Liam McArthur: We are looking for guidance.

Dr Macdonald: Obviously, that could go into statute. The key thing is that any framework, whether it be statutory or a non-statutory code of practice has to be developed in conjunction with all key players.

In talking about key players, I am talking about the police authorities, us as the data protection regulator, and colleagues in civil society, such as Big Brother Watch and the Open Rights Group. Including them will mean that we get proper representation of the arguments from all sides of the debate and we will come to some consensus. I do not think that I or Griff Ferris are going to get exactly what we want but we can certainly find areas of common ground.

Griff Ferris: It is worth saying that the way not to do it is what has happened in England and Wales and the fact that police forces have been given a free-for-all to do what they want with the technology. For the first 18 months, when asked, the Home Office said that it was a matter for the police. When fielding questions from members of Parliament, the minister for policing admitted that there is no legal basis for the technology—that is on the record—but the police were able to push ahead with the use of it.

The Biometrics Commissioner, the Surveillance Camera Commissioner, and even the Information Commissioner for a time, all said that it was not clear which of the many commissioners with their different remits had ultimate oversight of the technology. Although it did not quite fly under the radar as a result because it was known about and we and others were trying to talk about it, it did fly under the radar of effective oversight.

Although we do not believe that it should ever be used, the way to reach that would be to have a serious human rights analysis of the threat of this technology to human rights and civil liberties. How that can be done, I am not sure.

Liam McArthur: Mr Mukushi, do you have a view on whether, given all that we know about the way in which the technology is deployed, it can be compliant with human rights?

Tatora Mukushi: In Scotland, we have had the debate around the Scottish Biometrics Commissioner Bill, and a lot of expert advice has come out of that. That seems to be the right place and model. There should be a strict code of conduct with some enforcement powers to allow a biometrics commissioner to put in place rules and regulations about the use of such technology and to carry out the consulting and public engagement role that Dr Macdonald is talking about.

It is correct that the police would like to take those decisions, but they need to do so within the framework that the Parliament sets for acceptability and accountability.

I have my reservations and, as the technology stands, there is unfortunately far too much evidence of its failings as opposed to evidence of its real usefulness. However, that is a proportionality assessment and it really should be handled by Parliament. It should decide where that power sits, and that is part of this process. It will have to sit quite high in the public consciousness and I do not see anywhere apart from the Parliament to put it.

Liam McArthur: Thank you for the hospital pass.

James Kelly (Glasgow) (Lab): Throughout this meeting, there has been discussion about the legal basis for the use of live facial recognition technology and whether there is a proper legal basis or what can be done to establish one, and whether the use of the technology is proportionate.

To date, Police Scotland has not used the technology. Should it put on hold its use until there is a clear understanding of and consensus on the legal basis and proportionality of using it?

13:30

Dr Macdonald: One of the key requirements under the GDPR is that, whenever personal data is likely to be processed, a data protection impact assessment should be considered, particularly when the nature of the information is as sensitive as it is in this case. There is also a requirement that if, in undertaking the assessment, the data controller of the organisation—in this case, Police Scotland—identifies risks to the rights and freedoms of individuals that cannot be mitigated, they must consult the Information Commissioner's Office. That is one step. If they can convince us that, having done that, they have a legal basis—I understand that Police Scotland suggests that its duty under the Police and Fire Reform (Scotland) Act 2012 to "prevent and detect crime" might be appropriate—and have come up with suitable mitigation measures to protect the rights of individuals, that is fine. If the data controller does not do that, we can take action to prevent them going ahead.

I would not like to give a categorical yes or no in response to James Kelly's question, because it depends. However, we should be fully engaged with Police Scotland, which should come to us as a direct consultee and not as part of a public consultation. By law, it is required to come to us directly to discuss the matter.

Griff Ferris: There is such a huge weight of evidence, which the committee has heard or will have read about, against the use of the technology that it certainly should not be used at the moment, at the very least. However, we believe that live facial recognition technology should never be used by police in this country.

Matthew Rice: Looking down the list of institutions and individuals that have raised concerns about the continued roll-out or use of facial recognition—such as the House of Commons Science and Technology Committee, other MPs, civil society organisations and other regulators—it is self-evident that it would be foolish for Police Scotland to pursue it without clarifying what it means. We should be clear about whether we are talking about live facial recognition or post-event facial recognition, which is when data is captured and, after the fact, the technology is used to work something out.

At this stage, the Open Rights Group is of the same opinion as Big Brother Watch and a long list of other organisations that a moratorium on facial recognition is absolutely necessary. We would raise a highly sceptical eyebrow if Police Scotland went further down that line.

Tatora Mukushi: I agree that a moratorium would be appropriate. I cite the work that the Justice Sub-Committee on Policing has done on digital triage devices, which are known as cyberkiosks. What happened with that was that Police Scotland proceeded with a form of technology without doing impact assessments and so on, which has now delayed things for 18 months. That could have been averted by doing all the homework first, which would be an appropriate process to follow in this situation. Due to the fact that Police Scotland has not proceeded with the roll-out of facial recognition technology without hearing from other people, it seems that it is minded to hold off until more is known.

Rona Mackay (Strathkelvin and Bearsden) (SNP): I will touch on the accuracy and reliability of the technology, an issue that has already been raised. It has been suggested that the use of facial recognition technology can be subject to issues such as racial and gender bias. Should there be much more rigorous technical testing of the equipment? Does it concern you that it has already been picked up that the equipment has been far from accurate in many cases?

Griff Ferris: It is a very serious concern that this technology has been shown to be ineffective. Our original publications around its ineffectiveness were taken from freedom of information requests to the police which found that the Metropolitan Police's technology was 98 per cent inaccurate, while South Wales Police's use of the technology was 91 per cent inaccurate. That was in 2017 and we have not seen evidence to suggest that that has significantly changed. An independent report into the Metropolitan Police's use said that it was around 81 per cent: this is an incredibly inaccurate technology that misidentifies people at much higher rates than it identifies them.

Multiple academic studies have found that the technology discriminates against people of colour and women. Admittedly, the technology being used by the UK police has not been tested: the police have refused to put it through that testing and have refused our requests that they publish any reports of their internal review and testing. A few months ago, a member of the Metropolitan Police who is leading the implementation of its technology admitted that the Met is aware of significant gender bias, but has so far not told us of steps that it has taken to use it.

It is worth saying that, although it is extremely serious that this technology has those elements of discrimination and bias, even if they were not present we do not think that it would be compatible with human rights. Notwithstanding that, the fact that the technology has that discrimination bias

should be enough to disqualify its use on that ground alone.

Matthew Rice: That is a really pertinent question. It is great that we are having this debate in Scotland about what we would like to see in Scottish society, but the thing to keep in mind is that any facial recognition technology will more than likely come from a commercial provider that will have trained its system on some number of datasets. The problem begins in that lab, where they decide on this particular dataset with those particular people. The biases come out of that. From what I understand, it is almost impossible to walk back from that. We might discuss what accuracy level we want to look at, but it may never be achievable. That may not matter, either, from a human-rights compliant perspective.

We are in essence relying on another organisation's ethics and the decisions that it has taken in the development of its technology to determine whether it is ethical and accurate or encoded with the biases that we have seen so far. It is really important to bear it in mind that we are not in a vacuum or a silo here: we are relying on decisions taken by other people, and those decisions may not be in the control of Scottish society.

Tatora Mukushi: Taking the evidence that has been given as read, there is ample evidence of the failings in the technology. I think that should give rise to concerns about how Police Scotland uses its funding. If Police Scotland were to invest in technology that had this failure rate, there would rightly be a public outcry, because it is hardly effective or efficient.

When we talk about necessity and proportionality, we must think about these things in a budgeting sense. When public bodies are accounting and budgeting, they must have these things in mind, because this will be a vast amount of money that could easily be spent on something else more viable, more useful and with a proven efficacy rate. There should certainly be more rigorous testing but also, within the process of developing these technologies, there should be a more considered view of how they will be audited, more of a desire to see them audited and to say, "Look, here is the trail, here is how we have tested it and here is how we can show that it will work". And if they do not work, there should be a willingness to accept that they have not worked and that we must go back to our values.

Griff Ferris: I will give an example of how this technology can affect people in a very tangible way—I appreciate that something like this can often be a bit intangible. At a deployment of live facial recognition technology by the Metropolitan Police in east London that we were observing, a 14-year-old black schoolboy was stopped by plainclothes officers when he walked past the van where the camera was located. He was pulled on to a side street by four plainclothes officers who asked him what he was doing there. He was on his way home from school and he was wearing school uniform. He was questioned, asked for his phone and fingerprinted. It was only after they checked his fingerprints against those of the person who they believed he was that they realised that he was just an innocent schoolboy walking home.

That is just one example of how this oppressive and authoritarian technology can seriously impact people on the ground. An innocent 14-year-old boy who was walking home from school was swooped on by police who believed that he was an individual on their watch list, because the technology had said that that was who he was. He was subjected to a pretty harrowing ordeal.

Rona Mackay: There is also the point about the human operators' relationship to and connection with the technology. One person's perception of an image might be different from another's. Could that issue ever be resolved? Even if the technology were to become more advanced and more accurate, would there still be an element of risk, given that we would be depending on someone's judgment and perception?

Griff Ferris: The example that I gave shows that the technology made an inaccurate match, but the officers in the van looked at that and said, "It looks like him. It must be him. We should stop him." There was a failing not only by the technology, but by the officers. The two things are linked. The technology is inaccurate and biased because, as has been mentioned, the datasets on which it is trained are often biased. The datasets often contain a majority of white men, which is why the technology provides such a high level of misidentifications of people who are not white or who are not men. The technology is simply not able to recognise them. There is clearly an issue at both levels.

Dr Macdonald: The UK Information Commissioner raised concerns about the effectiveness of the technology and about groups in which there is a disproportionately high number of mismatches. Her view is that the technology should be deployed only when there is a low tolerance, which is obviously based on the biased data sets. However, the police need to work on the basis of the best evidence that they have.

Crucially, when police deploy the live facial recognition technology, they should review the outcomes as time goes on, so that we can look at how effective the technology becomes. Effectiveness is not just about the ratio of mismatches to images; it is about the final outcome and whether someone has been proven

guilty following their identification. It is an on-going educational issue and an on-going technological and statistical issue, and there is a need for continuous improvement.

Rona Mackay: What do you mean by "low tolerance"? I did not quite follow that.

Dr Macdonald: It relates to the proportion of mismatches. We have already identified that there is a disproportionately high level of mismatches of people of colour and of females, because the data sets are based on white males.

Rona Mackay: Thank you.

The Convener: I want to pick up on a point that Mr Rice raised. I stress my lack of technical know-how—which is important in this case, because not everyone in the community is an IT expert—but it seems to me that the police themselves will not devise the equipment; commercial operators will make the bits of equipment. It is like when all the different mobile phone providers tell us the various good things that their phone does and do not highlight any of the negatives.

It seems that, were the police to go ahead with the use of the technology, there would be a public procurement issue. How could the police make a judgment on that? We have heard previously about the models that other forces have used, and those models were well down the league table in terms of efficiency. I am not necessarily commending the acquisition of bits of equipment but, were the police to do so, how would they go about that? Manufacturers will be well aware that Police Scotland has laid out a long-term IT strategy that mentions such equipment, so they will know that Police Scotland is very much in the frame for buying. What parameters should be set? A manufacturer would not necessarily consider the human rights impact.

13:45

Matthew Rice: From my experience before I joined Open Rights Group, my understanding is that the private surveillance industry often thinks about sales rather than the rights impacts.

We have to think about the process sequentially. The worst-case scenario is what happened with the digital device triage system purchase, in which procurement was done before any assessment of the efficacy of the system or of the human rights impact and data protection compliance. The equipment then sat around for a number of months, and it continues to sit there. An intention to purchase equipment should not manifest in procurement before a wider public debate has taken place and a lawful basis, as well as the specific terms under which the technology will be used, have been established. Bear in mind our continued reluctance to accept that live facial recognition is necessary in Scotland, so I am talking about other forms of technology, but its use still needs to be defined in law before it becomes a matter for technology procurement.

We should reflect on the digital device triage system, or cyberkiosk debate in considering what the process should be and the sequence. The public, members of the Scottish Parliament, civil society organisations and other groups should be able to feed into that before we even begin to think about procurement.

Tatora Mukushi: I will reinforce something that one of your previous witnesses, Dr Bobak, said. I believe that a joint project between the University of Stirling, Imperial College London and another university is developing the technology with Government funding. With that sort of public process to develop the technology, we could build in human rights concerns and solutions at an early stage and develop the technology along those lines. To be honest, if the technology cannot be developed with those things in place, that is a good argument for not using it.

Griff Ferris: In our other work on information and human rights concerns relating to new uses of technology, we often find that technology is bought and then the authority that is attempting to use it tries to fit the framework around the technology, rather than first having high human rights or data protection standards in place and then looking to procure technology that fits those standards. It is often done the wrong way round.

Dr Macdonald: That almost takes us back to the comments right at the start on the retention of custody images. There is now a requirement to have privacy by design built into the process, and that includes procurement. If personal images are to be processed, the process should ensure that the equipment that is to be used will allow deletion and compliance. The issue has to be much further up people's agenda.

Margaret Mitchell (Central Scotland) (Con): I want to drill down a little into the issue of public consent and public engagement. It is clear from what we have heard that you do not think that public engagement has been sufficient to explain the purpose of using live facial recognition in open spaces, so this is almost a rhetorical question, but I will ask it anyway, just for the record. Should it be a prerequisite to carry out community, privacy and equalities impact assessments prior to the deployment of this technology in open spaces?

Matthew Rice: Yes, absolutely.

Griff Ferris: Absolutely, although those assessments on their own are not sufficient to give permission for the use of the technology.

Margaret Mitchell: That was what my next question was going to be about. What else can be done, if anything?

Dr Macdonald: As I explained, there is an absolute statutory duty to do the privacy part of that. Maybe assessments are one question on which we can all concur, although I can comment only on the DP side. It includes a public engagement element, because people must be aware of what is happening and what can go wrong with the technology. We probably need to have a much wider public debate.

Tatora Mukushi: Again, Dr Macdonald is correct. The only thing that I would add is that it is important to remember that, even when the public are informed, and perhaps surveys or polls have been done, there must be a human rights-based framework around the use of the technology. Even if the public were somehow seen to be signalling support to a degree for the technology, if it is not human rights compliant, there should not be a whitewash. It is not a competition between a democratic mandate and a human rights-based framework; the two have to go hand in hand.

Margaret Mitchell: I think, again, that the individual circumstances must be looked at. There cannot be a blanket application.

Tatora Mukushi: Absolutely.

Margaret Mitchell: It seems that no one has anything to add on public consent.

Jenny Gilruth (Mid Fife and Glenrothes) (SNP): Good afternoon. Following Margaret Mitchell's line of questioning and referring back to some of the answers to Liam McArthur, we know that facial recognition has been used at political events and campaign marches and rallies. What impact might it have on democracy if people think that they might be being watched for things that are entirely legal and legitimate? Do you think that facial recognition is a danger to democracy?

Tatora Mukushi: I point you to the submission to the inquiry from Dr Aston, who said that there is a dearth of information about the impact of increasingly technologically mediated interactions on police legitimacy. It is something that we have to be very concerned about. We have a culture of policing by consent in this country and, if we start having more and more interactions through cameras, websites and all the rest, we do not know what the long-term impacts will be. If we are going to risk that, there must be a very important proportionality assessment of doing things differently from how we have done them, which has been shown to work. The purpose of policing has to be, as well as detecting and fighting crime, enhancing safety and well-being. That is in the legislation, and policing must meet those requirements, as well as the requirement to detect crime.

Griff Ferris: It can certainly have a very serious impact. It is well established that surveillance can have a very serious impact on people's willingness or ability to exercise free expression, not least—and this is most pertinent—the use of live facial recognition at public events such as the peaceful, democratic protests that it was used at in south Wales. It certainly has a chilling effect. In the legal challenge that we brought alongside Baroness Jenny Jones, who is a long-standing campaigner on many issues, not least the environment, one of her many arguments was that it would severely impact her ability to go to political events and to meet people as part of her parliamentary work but also as part of her activism. She was extremely concerned that other people, such as whistleblowers, would be less willing to meet her to discuss serious and important disclosure and other issues if, as she is concerned they might, she and her work in democratic areas might be subject to this technology.

Matthew Rice: There has been some strong work on the chilling effect of online surveillance. Not only surveillance that is overtly proven but people having the feeling that they are being watched can cause them to change their activities and behaviours. PEN International has done very strong work on that. Facial recognition carries very similar hallmarks: if a person feels or understands that facial recognition may be being used, even if it is on a non-descript camera and is not being used, it changes their perception, or how they act, which potentially affects their rights to freedom of assembly and association and freedom of expression. It is very much like other forms of surveillance, and the chilling effect and the harm to democracy could be very real.

Dr Macdonald: As you will be aware, we produced a report following the European referendum on the abuse of data and the selling of personal data, and how that disrupts democracy. We would have similar fears if facial recognition technology were being used in ways that have such a chilling effect. Again, it comes down to the specification of when to deploy. Just doing a fishing exercise and identifying future action by some individuals would be entirely unacceptable and no doubt in breach of people's article 6 rights.

Jenny Gilruth: You will be aware that we are considering a bill to introduce a Scottish biometrics commissioner. Should consideration of live facial recognition and public confidence in its use be a priority for the commissioner?

Matthew Rice: Yes. It is clear that that is a hot topic and an issue of public concern. The public have had an instinctive reaction to that issue in any polling that has been done. Seeking to

establish public understanding of and trust and confidence in the use of biometrics in a policing context will be vital for the nascent role of the Scottish biometrics commissioner, and facial recognition is probably at the top of that list.

Griff Ferris: Over the past few years, the England and Wales biometrics commissioner has made several comments on the use of live facial recognition, but he does not have any power to do anything about it. I do not know the full extent of what is or is not proposed in introducing a Scottish biometrics commissioner or what powers they may or may not have, but it is worth including in the conversation the view that, just because the technology is available and other people are using it, that does not necessarily mean that it should be used. That has been lacking in the conversation in England and Wales—it has been thought that, just because the technology exists, it must therefore be used and regulated in some way. It should certainly be within the remit of an authority to say that the technology is not wanted and that it should not be used, for all the reasons that have been well discussed over the past hour.

Tatora Mukushi: I point to the work of the independent advisory group that researched the role of the proposed Scottish biometrics commissioner. It is clear that it had facial recognition in its sights, and it cited that as an area of concern.

I would not necessarily say that live facial recognition should be a priority. All emerging technologies will certainly be a priority. The chief priority is to establish a legal framework and a code of conduct giving guidance, certainty and transparency in relation to how agencies—whether they are public or private—are directed. Obviously, there has been a gap in respect of what has been said before the committees about the scope of the biometrics commissioner, particularly with regard to their powers and accountability. It is very important that the commissioner is positioned in a way that, whatever they do and whatever technology they look at—whether that is facial recognition, drones or cyberkiosks—they can lay down consistent and clear guidance. That is a priority for the commissioner.

Dr Macdonald: I add a note of caution. There is, of course, a potential overlap between our work in regulating the data protection side of things and the work of the Scottish biometrics commissioner. It is clearly laid out in the Scottish Biometrics Commissioner Bill that there is that distinction. We still have responsibility for enforcing people's rights. South of the border, there is also the Surveillance Camera Commissioner, of course. The more commissioners there are in a general area, the more opportunity there is for confusion. I think that facial recognition should be included in the Scottish biometrics commissioner's remit, but it should be borne in mind that we have a statutory role as the reserved regulator for data protection.

The Convener: The Justice Committee is picking up those issues.

Fulton MacGregor (Coatbridge and Chryston) (SNP): Good afternoon, panel. I want to ask about technological developments in the area that are driven by private companies. I know that the convener started to explore that issue, particularly with Matthew Rice, but do any of the panel members who did not get a chance to speak earlier have any concerns about the possible blurring of boundaries between the interests of private companies and the responsibilities of the police, particularly in relation to human rights? I know that we have touched on that issue already.

Griff Ferris: Across England and Wales, there has certainly been a blurring of the boundaries between the police and private companies. Although different police forces have used the technology since 2015, the fact that a number of private companies were using it came to widespread attention only around August this year. We investigated that and, when we initially sent freedom of information requests in 2017 and 2018, we were told by a number of police forces that they were not working in partnership with any external companies.

14:00

It came to light in August 2019 that the Metropolitan Police and the British Transport Police had shared images with and worked with the King's Cross estate in central London, which was using the technology. It came out that a number of other large public spaces, including a shopping centre in Sheffield and a music venue in south Wales, were using the technology in conjunction with various police forces, all of which had told us a year or 18 months previously that they were not working with external companies. That shows that there is a lack of transparency and knowledge about the situation. Potentially, there has been a deliberate element of secrecy to it, but there have certainly been close partnerships between the police and private companies that use the technology, all of which benefit the private companies that sell the technology, whether to public authorities or to other private companies that want to use it in their own spaces.

Fulton MacGregor: What might be the implications of such an arrangement for the person on the street? As you say, there might have been an element of secrecy about it. Why would there have been any need to be secretive?

Griff Ferris: It is extremely concerning that, as has been well established, the police have been

using the technology in a way that infringes human rights, despite all the supposed—yet lacking—safeguards around its use, as is the fact that private companies are able to use it secretly and without being held to the same high standards as public authorities.

It is difficult to speak at length without knowing what is going on. That is one of the problems—we do not know comprehensively who is using the technology and where. We have a few reports here and there of examples that organisations or journalists have been able to uncover, but it is difficult to say much, because we do not know.

In one example in central London, we know that the Metropolitan Police and the British Transport Police shared images with the King's Cross estate. We do not know whether anyone was stopped or removed from the area, but there has been an indication that the images were used to combat antisocial behaviour. We also know that some of the images that were shared were of people who had criminal records but who were not wanted for any crimes at that time. That suggests an expansion of the use of the technology, if it is just being used to monitor, track and, ultimately, control the movements of people who are or might be known to the police, but who have not done anything wrong in the present moment.

Fulton MacGregor: Should a legal framework explicitly refer to the people who have responsibility for capturing, storing and deleting images from live facial recognition technology?

Matthew Rice: Yes. It is necessary to reflect that the technology does not exist only in the policing context. In a specifically Scottish context, we know that Glasgow City Council has a number of closed-circuit television cameras, because it replied to the committee's consultation. In its response, the council sought to explain the council using the technology versus Police Scotland using it. It seems to be that there is some ad hoc organisation: the council seems to recognise that information being moved from Glasgow City Council—which is a public authority—into a policing context would place it in a different legal framework and would require a separate and additional basis for using it.

That is good, but it should be straightened out in clear primary legislation how information sharing and direct use of the technology should work. That is not about just the output from the technology: it is also about, say, Police Scotland being able to view monitors and so on as the technology is being used, which is slightly different to sharing information that is derived from the technology. All of that needs to be clearly articulated in law.

The individual cannot see where the boundaries are in terms of interference and autonomy when they are walking down a street in Glasgow or are walking around their housing association estate, because they do not know where the images that are being collected could end up. Ultimately, we need to provide the public with clarity about what happens when they walk down the street. It might seem to be strange that explaining to the public what will happen when they walk down the street is the burden, but the more such technologies move into other sectors, the more we will have reckon with that.

Tatora Mukushi: There are probably two separate strands, one of which involves private organisations acting as proxies for public authorities. Whether such organisations gather data specifically at the behest of a public authority or gather it in the knowledge that it is reasonably foreseeable that it will be used by a public authority, they should have in mind the same human rights standards, which should flow from the legislation—article 6 of the European convention on human rights, which is incorporated in the Human Rights Act 1998. They should be bound by that and should comply with the same requirements for assessments and evaluation.

The other strand involves private organisations simply using data for their own purposes, whatever those might be. I am not entirely a data protection expert, but I understand that some of that would fall within the remit of the Information Commissioner, because it would be data that has been collected and processed. Images are still data and must be governed by the same rules about collection being strictly necessary and about how they are used. Although that might fall outwith the human rights argument, there is perhaps a need for the Scottish Government, as Matthew Rice said, to make a statement of values about where the boundaries lie in our society, and to say that any organisation that uses biometric data should be held to a higher standard, because of the nature of biometric data. Its use has the capacity to intrude severely on people's lives, so private organisations should be held to a higher standard than they normally would be.

Griff Ferris: Although private companies might not have the same powers as public authorities such as the police, they are much more likely to have a lower threshold for use of the powers that they have. That might involve using facial recognition technology for barring from shopping centres people who have shoplifted from them, or for barring from public spaces, or even public-private spaces, people who have engaged in antisocial behaviour. Private companies' barring of people from going to shops because of a misdemeanour that was committed in the past is just as chilling and authoritarian as use of such technology by the police.

For what it is worth, the declaration that was agreed on by 26 rights groups and a number of leading parliamentarians included a moratorium that would cover use of live facial recognition by not just the police, but private companies.

Dr Macdonald: When it comes to the relationship between the police and private providers, our concern is about how that fits in with the GDPR framework. There needs to be a clear contract between the two parties, especially when a party acts as processor on behalf of the police. That contract should refer to the usual provisions on security and so on. One of the benefits of the GDPR is that, whereas breaches by a processor were previously deemed to be the responsibility of the original controller—which meant that regulatory action would have been focused on, say, Police Scotland, when one of its controllers was in breach—under the new framework, the processor could have regulatory action taken against them. That provides a spur to processors to ensure that they comply.

As Griff Ferris said, the situation is slightly different when the private sector does the processing itself. The "strictly necessary" requirement under part 3 of the Data Protection Act 2018 is all to do with processing for law enforcement purposes by competent authorities, of which the police are one. In some cases, councils are competent authorities. However, as Griff Ferris said, the private sector has lower thresholds.

Liam McArthur: I am conscious that I am matching the convener stride for stride in exposing my lack of insight into the technology. Matthew Rice mentioned use of CCTV, which I suppose would be deployed to discourage and to pre-empt, in a sense. However, the technology appears to be being used to support cases being brought without there being the same level of concerns in relation to the reliability of live facial recognition. Is there any reason why that should be the case?

Matthew Rice: Could you repeat that?

Liam McArthur: You use CCTV evidence to demonstrate that an individual was in a location at a particular time in order to support a criminal case, or whatever it is, as it goes through the legal process. There seems to be an acceptance of the reliability of such evidence in the same way as, from the figures that you have given, there is of the reliability of live facial recognition technology. Is there a reason for that?

Matthew Rice: I will need to dip into the Scottish criminal law seminars that I attended years ago. Other corroborating evidence would be required. For example, we might know that X was in a certain area and was wearing certain clothes. The problem with live facial recognition is that, in essence, it is an analysis of an individual's face and facial features up to a mathematical point at which it can be said that they are quite like those of a certain individual. It does not necessarily have all the corroborating features around it. Using it in the context to which Griff Ferris referred—when a person is immediately detained—is quite different from the context of a person being prosecuted. When a person is prosecuted, a series of decisions have been made on the basis of the evidence that is immediately available and the likelihood of prosecution, whereas a 14-year-old black child might be detained because he matches mathematically on the basis of a dodgy data set or a dodgy algorithm. That is the stark contrast that we face.

The Convener: Thank you very much for your evidence. It has been extremely helpful to us.

14:11

Meeting suspended.

14:13

On resuming—

Scottish Crime and Drug Enforcement Agency

The Convener: Our next item of business is consideration of the Metropolitan Police Service's recent peer review of Police Scotland's anti-corruption unit's investigation of the former Scottish Crime and Drug Enforcement Agency. I refer members to paper 4, which is a note from the clerk, and to paper 5, which is a private paper.

As members will be aware, there are live court proceedings in relation to the case, so I draw their attention to standing orders rule 7.5, on sub judice issues—I am sure that members know the rule word perfect—and ask them to be mindful of that when they make any remarks on the record.

I invite members to give their views on the Metropolitan Police Service's recent peer review.

Liam McArthur: There is a suggestion that you could, on behalf of the sub-committee, write to the Scottish Police Authority to ask whether consideration has concluded. There are probably a number of detailed questions that we will want to fold into that request, but that seems to be a sensible way of proceeding.

The Convener: We will write to the SPA to seek clarification of whether its consideration of the issue has concluded. We will ask a range of questions and, as ever, the letter will be published on our website. Do members agree?

Members *indicated agreement.*

14:15

Meeting continued in private until 14:26.

Published in Edinburgh by the Scottish Parliamentary Corporate Body, the Scottish Parliament, Edinburgh, EH99 1SP

All documents are available on
the Scottish Parliament website at:

www.parliament.scot

Information on non-endorsed print suppliers
is available here:

www.parliament.scot/documents

For information on the Scottish Parliament contact
Public Information on:

Telephone: 0131 348 5000
Textphone: 0800 092 7100
Email: sp.info@parliament.scot

The Scottish Parliament
Pàrlamaid na h-Alba