OFFICIAL REPORT
AITHISG OIFIGEIL

Justice Sub-Committee on Policing

Thursday 21 November 2019

Session 5

The Scottish Parliament
Pàrlamaid na h-Alba

Thursday 21 November 2019

CONTENTS

JUSTICE SUB-COMMITTEE ON POLICING
10th 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:

Dr Anna Bobak (University of Stirling)
Dr Christopher Lawless (Durham University)
Dr Joe Purshouse (University of East Anglia)

CLERK TO THE COMMITTEE

Diane Barr

LOCATION

The David Livingstone Room (CR6)

Scottish Parliament

Justice Sub-Committee on Policing

Thursday 21 November 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 10th meeting in 2019 of the Justice Sub-Committee on Policing. We have apologies from Jenny Gilruth, who has another piece of parliamentary business to deal with.

Agenda item 1 is a decision on whether to take in private agenda item 3, under which we will consider the evidence that we will hear today. Do members agree to take agenda item 3 in private?

Members *indicated agreement.*

Facial Recognition Technology

13:00

The Convener: Agenda item 2 is an evidence session on how policing in Scotland makes use of facial recognition technology. I refer members to paper 1, which is a note by the clerk, and paper 2, which is a private paper.

I welcome the witnesses to the meeting and thank them for their written submissions. Dr Christopher Lawless is an associate professor at the department of sociology, Durham University; Dr Joe Purshouse is a lecturer in criminal law at the University of East Anglia's law school; and Dr Anna Bobak is a postdoctoral research fellow in psychology at the University of Stirling.

I will kick off with a question about the legal framework. Will the panel comment on the legal framework—if there is one—that forms the basis of how facial recognition technology is used by police forces elsewhere in the United Kingdom?

Dr Joe Purshouse (University of East Anglia): That topic has recently been considered by the High Court in England and Wales in the case of R (on the application of Bridges) v Chief Constable of South Wales Police. There are—

The Convener: I interrupt to say that it is appropriate that we talk about that—indeed, I was going to ask about it—but people will be aware that there is potential for an appeal, so some aspects may be sub judice. I am sure that you will be alert to that.

Dr Purshouse: Absolutely.

There are essentially two issues to consider in deciding whether a legal framework is in place and whether that framework is adequately prescribed to regulate the use of facial recognition technology. The first issue is whether there is an enabling power to use the technology. The Home Office and the police forces that have trialled the technology tend to suggest that the enabling power is in the common law, in cases such as Rice v Connolly. Basically, it is a general police power to prevent and detect crime that gives the basis for using the technology. Whether that provides a sufficient legal basis or power to use the technology might be questioned.

The common-law decisions that created that power were quite general in their terms and were made when the technology was not really developed. In English law, generally a distinction is drawn between physical intrusions, such as assaults and searches that police officers might have to make—they would be assaults but for a legal basis—and informational intrusions. The way that the existence of the power has been justified

in England and Wales is that informational intrusions require only a general common-law power, whereas physical intrusions require a statutory power. There is controversy over that—I think that the issue will get more controversial in future—because, as surveillance technologies advance, they enable the police and other public bodies to do more intrusive things without actually interfering physically with an individual. Therefore, it is questionable whether such a broad general power can adequately permit the police to use the technology.

The second point is about the existence of a legal basis that is sufficiently precise to regulate a public authority's discretion in using the technology. The police forces that have trialled such technology tend to rely on a broad range of subsidiary or implicit powers. For example, to some extent, data protection legislation regulates the use of facial recognition technology, as do human rights provisions and the Police and Criminal Evidence Act 1984. The question is whether they confer on the police too much discretion in deciding the exact parameters of what constitutes acceptable use of the technology. I am sure that we could go into that further if the committee wishes.

The Convener: Yes—there will be a lot more questions. Thank you very much.

Dr Christopher Lawless (Durham University): In England and Wales, there is the Protection of Freedoms Act 2012, but that covers only certain forms of biometric data, which, if I recall correctly, include DNA, fingerprints and footprints. It concerns me that there has not been any clearer or more direct legislation on facial data. I am aware of concerns about the police's approaches to collecting such data in England and Wales, where there seems to be not much of a system and there has been a fairly unregulated approach to the collection of images. That leads me to wonder whether the Protection of Freedoms Act 2012 could be made clearer on facial data or could be extended to cover facial images explicitly.

Dr Anna Bobak (University of Stirling): I am not a legal expert, so I will refrain from adding to what Dr Purshouse and Dr Lawless have said on that point.

I am aware that the Scottish police have their own way of archiving facial data. I believe that custody images are not retained in the police national database unless someone has been charged and convicted within six months so, in that respect, Police Scotland is ahead of its English colleagues.

The Convener: Thank you. We might touch on aspects of that.

I want to ask our witnesses, in very broad-brush terms, about the Welsh case. I presume that the police force there felt that it had met the criteria of necessity and proportionality. Do you have a view on that? Do you envisage similar challenges in Scotland were such technology to be put in place here?

Dr Lawless: Again, I will give my response in the broadest terms. I speak as someone who is not a legal expert but who takes a professional interest in judgments on such matters, so it is probably best if I leave it to the other panellists to speak about the legal intricacies of such cases. However, they make me think that we need to be attuned to further challenges.

When I read the judgment in the Welsh case, I wondered what would have happened had the individual been directly impacted by facial recognition—perhaps through finding that they had been on a watch list or suffering adverse consequences as a result of a false positive identification. That led me to wonder whether there could be similar challenges in future. For me, the situation depends on individual circumstances and how facial recognition technology, which could be very different in all sorts of ways, is engaged with.

Dr Purshouse: I echo Dr Lawless's view that the Welsh case involved a limited challenge and referred to a specific context, especially on the necessity of the measures. Necessity and proportionality are very broad questions. Human rights law offers a process for structuring analysis of where a balance should be struck between the benefits or potential benefits and the harms or potential harms of using such technology. That raises complex questions, which might sometimes require political judgment. However, it is important to remember that it is for those who are interfering with those rights, or purporting to do so, to justify the use of such technology as necessary and proportionate. Human rights law sets out that the use of the technology must have some significant benefit that could not be achieved through less intrusive means, and that the cost benefit should be worth while.

There are serious question marks over the trials of live facial recognition technology with regard to exactly how accurate the technology is and whether it has the potential to discriminate against certain communities. There are also questions around the broader social consequences, not just for individuals who are scanned but in the context of how the technology may change the way in which we relate to publicly accessible spaces, especially if we are taking part in a protest or attending a football match. Ultimately, it could damage the legitimacy of the police if it is seen to be an intrusive technology that has been rolled out

in ways that the public do not necessarily understand or trust.

Dr Bobak: I will say a bit more about the quality of the technology and how that might have an impact and present further challenges—

The Convener: We will come on to those questions, so I will stop you there. We will welcome your comments later.

I am not asking the panel to speak on behalf of the constabularies that have deployed the equipment, but is it your understanding that they will have made any sort of assessment in which they will have weighed up the constant tension between individual liberties and the perception that deploying such equipment will enhance community safety? I am thinking of a risk assessment, human rights assessment or community impact assessment—call it what you will. Has that been made apparent in public at all?

Dr Lawless: My understanding is that they have had to conduct certain assessments, including a data privacy impact assessment and an equality impact assessment. There has been some forethought. I got the impression that there was perhaps a little concern about how thorough the forces had been—I am talking more specifically about South Wales Police; I cannot comment very much on the Metropolitan Police. It seems that there was at least some effort to try to meet the stipulated criteria. I do not know whether colleagues can offer any more detail on that.

Dr Bobak: I am not sure about the assessment procedures, but my understanding is that the Metropolitan Police engaged with the public during the trials and that the public were informed that the trials were being conducted—the police handed out leaflets and spoke to the public about the use of live facial recognition technology.

The Convener: Members have a number of questions to follow up on some of the points that have been made.

Liam McArthur (Orkney Islands) (LD): To follow up on what has been said about the use of live facial recognition technology, Police Scotland has made it clear that it has not trialled such technology to date, but it is equally clear from the document "Policing 2026: Our 10 year strategy for policing in Scotland" that it is anticipating deployment during that period. I think that it is fair to say that Police Scotland has some anxieties about the functionality of such technology and it has accepted that some of the legalities could require greater clarification.

What is your view on the importance of getting the legal framework right from the outset? How would you anticipate that Police Scotland would best go about obtaining that legal clarity?

Dr Lawless: There is a very nice quote that another written submission used from Professor Paul Wiles, who is the Commissioner for the Retention and Use of Biometric Material for England and Wales. He said:

> "bolting on governance rules after technical development is much costlier than developing technical solutions within known rules."

I very much agree with that statement. It is good to have clear guidelines and a clear understanding before the technology is deployed.

I have read the "Policing 2026" document, so I understand that there is a kind of vision around the proposals, but I feel that we should institute a Scottish biometrics commissioner first, so that we have the role in place, with a code of practice at least formulated—such codes can be reviewed—and with the advisory systems in place, before face recognition is considered and trialled. It is important to have the framework before the technology is used, so that there is an understanding on the part of the police of the rules within which they can manoeuvre.

13:15

Liam McArthur: Given the level of public debate that already exists around live facial recognition technology, would that need to be a priority area for the incoming biometrics commissioner?

Dr Lawless: I think so, yes. There needs to be an appropriately rigorous public engagement process. I can talk a little bit more about that.

Surveys have been carried out by the Ada Lovelace Institute and the London Policing Ethics Panel, so we have some data on public attitudes, although it is limited. As with any poll, we should be careful not to take one poll as the last word. However, if we had a number of pieces of public research and surveys, we could perhaps start to discern a trend. The study that was carried out by Cardiff University also contained some data on public attitudes.

I sense that, so far, the public's view has been positive but very mixed. There is some support for facial recognition, but that varies, depending on what it might be intended to be used for. It seems from the limited surveys that have been done that there is more support for using facial recognition in connection with serious crimes, but less support for using it for more minor crimes. I thought that it was interesting that, whereas there was majority public support overall, according to the London Policing Ethics Panel report, there was significant opposition among the younger age group. Such factors need to taken into account.

The priority is to have a public engagement exercise, and that could involve similar kinds of surveys. I wonder whether the question is perhaps one for a citizens jury framework. It has been interesting to read some of the reflections about citizens juries. One survey participant spoke about how the boundary between experts and citizens is more blurred than we might think. Members of the public can bring their own experiences to bear on such questions in some quite informed ways. There is always the difficult question of what constitutes public approval, but the least that could be done is to utilise all possible public engagement methods.

Dr Purshouse: If I may, convener—

The Convener: I am sorry, but I think that Margaret Mitchell wants to come in.

Margaret Mitchell (Central Scotland) (Con): I have a related question. The discussion was moving on to public consent, as well as public engagement. Should the technology have community and human rights assessments attached to it, so that there really is a proper legal basis for it? I suppose that that is consent, in a way.

Dr Purshouse: Absolutely. On public opinion and human rights, and the relationship between them, I would say that public opinion on, and public support for, the use of technology are important. If that support is not there, that is a strong barrier against using it. However, that is not the end of the matter. It is worth remembering that human rights are there to protect vulnerable minorities. As Christopher Lawless alluded to, the surveys show that the demographics that tend to be subject to policing more frequently are less supportive of the use of technology, and that should be acknowledged in any breakdown of public support.

I go back to what Scotland should do in approaching the question whether to use the technology. There is an issue of putting the horse before the cart here. It is important to have an idea of the rules that should be in place, to research the impact of the technology on both individuals and society as whole and to have a broad debate about its proper limits before using it.

During the trials of the technology in England and Wales, there were inconsistent practices between the forces and private organisations that decided to trial it. Some organisations that use the technology decided that it was appropriate to gather images from multiple sources, while others restricted themselves to the use of custody images. Some decided to pursue non-criminal infractions and antisocial behaviour, while others focused on strict criminality. That inconsistency, along with some of the problematic practices, might have been avoided if we had held a broader debate and put some rules in place before rolling out the use of the technology. We could have decided whether it is a tool that should be reserved for the most serious crimes or one that should be used more broadly.

Margaret Mitchell: To be clear, would its use more broadly mean giving carte blanche to its use in open spaces? Would its use be as wide as that, or would we need to refine things in any way, so that there would be a prerequisite before deployment? How precise would we have to be?

Dr Purshouse: In our written submission, my colleagues and I recommended a moratorium on the use of the technology. That is particularly important in relation to public spaces. Essentially, that would mean pausing or blocking the use of the technology until the case is made that there are clear uses for it, that the dangers of demographic bias have been properly mitigated and that it can be closely regulated so that its use is truly proportionate.

Dr Bobak: It is incredibly important that special cases are very carefully considered. For example, how would police or law enforcement agencies deal with data taken from children or scanning those who are underage? How would they deal with any of the situations in public spaces that have been talked about, in which the search is not focused and someone might pop up?

Further, how would we regulate the competence of people who sit at the other end of the software—those who operate facial recognition technology? We know that, at the end of the day, it is the human who makes the decision and gets a candidate list of potential matches from the technology, and we know that human face recognition is extremely fallible. If someone is presented with an image from the software and a potential candidate list from the police database, they have to make a decision about how to proceed. It is incredibly important to ensure that those people's natural face recognition ability allows them to correctly make decisions about whether to proceed.

Dr Lawless: When we talk about proportionality, the important issue is the specific purposes for which facial recognition technology might be used, which need to be expressed as clearly as possible. That is the key issue in determining proportionality.

Liam McArthur: The witnesses have been very clear about the need to get the framework in place before roll-out. The arguments for that approach seem very reasonable.

We have done a compare and contrast between what is happening south of the border and what is happening in Scotland. Are there any jurisdictions

that are ahead of the game in terms of that broader framework? The more detailed and granular you try to make the framework, the more you risk running up against problems, because the development of the technology and the way in which it is used cannot be anticipated. Should we be looking to any other parts of the world for clues as to what the framework might look like?

Dr Purshouse: I do not know of any jurisdiction that is that far ahead with the technology and has developed a framework and then started to use it. The picture internationally is that some jurisdictions have a free rein on facial recognition surveillance and are determined to roll it out as far and as wide as possible. I am sure that that is not a model that Scotland would want to follow. Others are rolling out the technology and already have some broader regulations that they rely on to govern its use—England and Wales might be a model for that.

Others are at the point of considering the appropriate parameters of facial recognition surveillance and the extent to which there is a democratic mandate for its use before rolling it out. New Zealand is a good example of that. I am part of a funded project that is looking at the regulations in New Zealand, where facial recognition is being used in quite a limited way—similar to the position in Scotland—and where they are thinking about what needs to be in place before the technology is put to use.

The Convener: If you have further information on the experience in New Zealand, we would welcome that.

Dr Purshouse: I would be happy to follow that up.

Rona Mackay (Strathkelvin and Bearsden) (SNP): I want to ask about the accuracy and reliability of the technology, which has already been touched on a wee bit. Studies have shown that the technology used in live facial recognition can be subject to issues such as racial and gender bias, which can lead to many false positives when matching images to watch lists. Can you expand on that issue and how such problems could be rectified? It is clearly a serious issue.

Dr Bobak: I am happy to answer that.

Ethnic and gender bias is not an issue that is inherent in the technology; it is realised purely through the training sets that are used to train the algorithms. The training set of images is what the algorithm is trained on and the test set is what it is tested on. If the training set is predominantly Caucasian men, the algorithm will be biased towards higher accuracy for those types of faces.

The approach to regulation and quality assurance should consider the population that the facial recognition system will be used in and ensure that the training sets are reflective of the population set to avoid such bias. The issues can be rectified.

I am not sure whether the committee is aware of this, but the National Institute of Standards and Technology in the United States is a public body that has a continuous vendor test, where companies submit their algorithms for testing as frequently as every four months. That gives an idea of how fast the technology in the field is developing.

I was looking at the most recent test, and the company that provides the technology for the Metropolitan Police and South Wales Police does not use the top 20 performing algorithms.

There are ways to assess quality, for example by looking at the tests, but it is important that there is scrutiny of how public money is invested. I believe that it is public information that NEC is the company that the police in England and Wales use, and I have not seen NEC performing well in the tests in the last few releases of the test reports.

Dr Lawless: Looking at the experience of facial recognition in England and Wales so far, I am concerned that the police are reliant on commercial technology. The products that they use seem to be off the shelf, and questions arise about how fit for purpose the algorithms are. South Wales Police had a considerable learning curve in understanding the vagaries of the technology and how to set thresholds for determining matches and so on. There was a lot of learning and variation in relation to how the technology can be used.

One concern was that the police found that one of the algorithms that they were using made inaccurate categorisations, for example in relation to gender identification. The operators simply had to live with that—they did not seem to have much opportunity to shape the technology.

That is a general concern, but it leads me to think, in general terms and not just in relation to facial recognition software, that the police need to be quite wary about the claims that some of the technology providers make. We need to have an open conversation between the suppliers and the users.

Rona Mackay: As a non-technical person I did not even know that algorithms were involved. I know that that means that they are computer generated. Does that not raise quite a few questions? Is the same software used throughout, or do individual forces and areas get to choose? Who chooses what software to use, and who evaluates it to see whether it is fit for purpose?

13:30

Dr Lawless: My understanding is that South Wales Police gained Home Office funding to invest in facial recognition technology. I believe that the services were put out to tender for companies to bid for. It just so happens that NEC was successful. That is what I understand the process was in that case.

Rona Mackay: Do you envisage that the technology would be standardised in Scotland? Will it be one piece of software that is used and evaluated? Given that we are aware that there are problems, surely it needs to be as accurate as it can be.

Dr Lawless: It seems to me that police forces will inevitably have to rely on commercial providers for this technology. If a Scottish biometrics commissioner were to be instituted, there is a question about the kinds of conversations that would need to be had between potential providers and their customers. That could involve some quite awkward questions about how much commercial providers are willing to disclose, but I think that there needs to be a way of agreeing some basic standards and expectations.

Rona Mackay: That is really what I was getting at: there surely has to be some benchmark that providers have to reach. Dr Bobak mentioned the human element to the relationship, in matching and so on. Are you confident that that is of a high enough standard? It is obviously crucial.

Dr Bobak: Do you mean human performance?

Rona Mackay: Yes.

Dr Bobak: What we know is that human face recognition and the matching ability for unfamiliar faces—faces we do not know personally as those of colleagues, family or friends—are on a continuum. Some people are very bad at recognising faces, most of us are somewhere in the middle and some people are at the top end of the distribution, if you can imagine it in that way. Ideally, we would want to make sure that the people who operate the software are at the top end of the distribution; otherwise, it can lead to all sorts of problems.

I have something to add on the technology question. I believe that both South Wales Police and the Metropolitan Police use the same software from NEC, which is a Japanese company—I think that the software is called NeoFace Watch. Although I am not aware of the exact ins and outs of how the software was acquired, I was at a Home Office expo where companies advertised their services to the Home Office and the police, and NEC was certainly there. It would be extremely useful, for quality assurance purposes and for making sure that the top algorithms are used, to invite independent academic computer scientists to the table. They could mediate between police forces or law enforcement agencies that would like to acquire such software and private sector companies.

The development of algorithms is not restricted to the private sector. For example, research councils fund the development of facial recognition software and the University of Stirling, Imperial College London and the University of Surrey share a computer science grant. There is public interest and a public stake in developing top-performing algorithms. My main point is that it would be extremely useful to have a computer scientist at the table, taking part in legislation and quality assurance.

Liam McArthur: Concerns have been expressed about Police Scotland's use of the UK police national database in storing images and whether the rules around retention periods and so on are adhered to, particularly when it comes to images of those who are not subsequently convicted of a crime. Do you share those concerns? How would you address them?

Dr Purshouse: Those are very real concerns. To give you a brief bit of the history, there was a High Court case about the retention of custody images of people who had been arrested but ultimately not convicted of an offence. The UK Government's blanket policy at the time was deemed to be inadequate. It did not meet the requirements under article 8 of the European convention on human rights, and the wide retention of images was disproportionate.

Since then, the Home Office has implemented a policy under which an arrestee who has not been convicted but whose image has been retained can apply to have the image taken off the database. People do not really know about that policy because it has not been well publicised, and the take-up of that option is very low.

Hundreds of thousands—if not millions—of images have been retained and continue to be retained years after cases have been disposed of without a conviction. All those images are on the police national database. It is important that Police Scotland is aware of that and that a system is in place to manage whether Police Scotland can have access to, or potentially use, images that have been stored latently in a facial recognition system long after someone was involved in a criminal process but was not convicted.

It is an intrusion of privacy to retain a custody image of someone—an innocent person—on a profile long after the case has been disposed of. However, it is another thing to then add to the intrusion of privacy by further processing the image using a facial recognition system or,

potentially, by conscripting that person into a virtual police line-up. The issue needs to be managed, but I do not know how that would be done technically.

Liam McArthur: I might be oversimplifying the situation, but in terms of closure of a case in which someone has not been convicted, Police Scotland would be better placed than anybody to know what images have been sent for storage and would therefore be best placed to request their deletion. Is there complexity in that process to which I, as a layperson, am not privy, or would the process be, to your mind, fairly straightforward?

Dr Purshouse: I am sorry. Can you rephrase the question?

Liam McArthur: When a case is closed after court proceedings have taken place and the accused has been found not guilty, or after a decision is made not to proceed with a case, Police Scotland will be in a position to know what images have been sent to the national database for storage. I assume that Police Scotland would be best placed to request their deletion, as part of wrapping up the case. Is there complexity in that that is not immediately obvious, or do you see the process as being fairly straightforward?

Dr Purshouse: I think that that would be fairly straightforward. The Scottish approach—time-limited retention and not retaining images when there has been a non-conviction disposal—is important. Big Brother Watch's submission with the Open Rights Group makes the point that images of non-convicted persons that historically have been uploaded might continue to be retained on Scottish databases, so the sub-committee might want to look into that. If Scottish police use facial recognition software on the police national database, which contains images of many non-convicted people across England, Wales and Scotland, there is potential for intrusion. The biometrics commissioner might want to look at how the system is managed.

Dr Lawless: I have been thinking about that question. I imagined a scenario in which Police Scotland was investigating a serious crime and found a match on the PND of a person from England or Wales whose image had been retained but who was innocent or had not been convicted or charged. What would happen legally if that person was prosecuted in Scotland? Would there be grounds for appeal? Is that scenario another argument for extending the Protection of Freedoms Act 2012 for England and Wales to include provisions on facial data?

Perhaps there should be a retention regime similar to that for DNA. However, that would depend very much on England and Wales making such changes. What could Police Scotland do in relation to its guidelines for comparing images that are in the PND? The best answer that I can come up with is that perhaps Police Scotland could, in such scenarios, act as though the 2012 act applies to facial images. That could be one way of maintaining some consistency, for the time being.

Liam McArthur: There is a risk that, even if a match is 100 per cent reliable—or it reaches whatever the threshold is—inappropriate retention of the image would render it inadmissible as evidence. Someone could walk free on such a technicality.

Dr Lawless: It seems to me that that could be challenged or appealed.

Dr Purshouse: That could be contentious: I do not know enough about the admissibility rules in Scotland to give a firm view, but such an image would be admitted as evidence in England and Wales. Nonetheless, there is a general privacy risk that might not be easy to resolve. I appreciate that it might not be within the remit of Scottish lawmakers to resolve that problem, because England and Wales would retain the images. That is perhaps something to be mindful of when setting policies in this area.

Dr Bobak: I have two points to add. First, I believe that retention of images in the PND has been challenged in the courts, and it has been deemed to be unlawful to keep images of people who have been proclaimed to be innocent. There are technical issues with regard to deletion of such images, but that problem might partially solve itself once the technical issues were resolved and unlawful images deleted.

With regard to admissibility as evidence in England, I spoke to the Metropolitan Police about the matter last week. My understanding is that two types of image—evidence and intelligence—may be collected. If there is a potential match, but there is no one at the human end who knows the person in question personally—for example, a police constable who has previously arrested the person—and can verify it, the image cannot be presented as evidence in court, and can be treated only as intelligence. However, if a match can be verified by someone who knows the person—for instance, a police constable who can identify them because they have arrested them three times—the image might be deemed to be admissible as evidence. It would be referred to as being "PACE code D compliant", because it would comply with code of practice D under the Police and Criminal Evidence Act 1984.

Margaret Mitchell: I want to probe further on whether such an image would be admissible in court. The committee heard in evidence from the Crown Office and Procurator Fiscal Service that there being no legal basis for retention would not

necessarily make it inadmissible. The prosecutor would consider fairness, and the court would look at the facts and circumstances in each case. Do you see the process operating in that way in general? Is it sufficient? Should more be done, or are the checks and balances adequate?

Dr Purshouse: The process operates in a similar way in English courts; there is a balance between the probative value of the evidence and its pre-prejudicial effect. The questions are, do the ends justify the means, and should the evidence be admitted anyway?

It sounds as though you are describing a similar rule in Scotland. It is a difficult and complicated issue, with a lot of arguments on either side that might take the committee quite far away from the focus of its inquiry.

Margaret Mitchell: I suppose that "fairness" is subjective.

Dr Purshouse: There is subjectivity to fairness, and there are different schools of thought with regard to whether courts should ever admit improperly obtained evidence. Should it all be admitted or—this is the view to which I subscribe—should the correct balance be somewhere in the middle?

We do not want to jeopardise or collapse serious prosecutions, in which there is strong, credible and reliable evidence, because of a very minor technical procedural oversight. It is right that there is a balance to be struck, but the question of where we strike that balance is very difficult, and there is—as you say—an element of subjectivity.

James Kelly (Glasgow) (Lab): I want to explore the issue of live facial recognition technology being used at public events such as political rallies, marches and football matches. Is there a danger that such use could make the people who are present at such events feel as though their right to freedom of expression is being compromised or undermined?

13:45

Dr Purshouse: The short answer is yes, but I will elaborate a little.

Where such technology has been rolled out at football matches, we have seen fans and their association groups being really quite resistant to it. At a match between Cardiff City and Swansea City in the South Wales Police area a couple of months ago, we saw in-stadium protests by fans taking place. I believe that fan groups here also objected when use of live facial recognition technology at football matches was proposed in Scotland. The use of such technology could have a chilling effect and could harm relationships between the police and groups such as football fans, between whom there might already be historical tensions. If such surveillance were to be seen as unjustified or oppressive, it would not have the desired effect of building trust or confidence between those groups

Some of that concern carries over to protest movements. A growing body of empirical research suggests that when overt surveillance is used at marches by legitimate non-violent protest groups, it can harm and chill their activities. When a surveillance camera van arrives, the perceived legitimacy of such groups in the eyes of the public can be damaged, and they might then struggle to generate resources and public support.

Therefore, use of such technology is a risk. It might be proportionate in some circumstances—I do not want to express a strong view on whether it could ever be completely proportionate—but it certainly needs to be mitigated and managed.

Dr Lawless: I will follow on from what Dr Purshouse said about political demonstrations. Measurement of any chilling effect is difficult, because it would be hard to evaluate how many people might have chosen to stay away because of the presence of cameras.

However, I share the general concerns that have been expressed about how people might respond to the presence of facial recognition technology. We must also take account of the famous strand in sociology that argues that if we know that we are under surveillance we manage our behaviour according to that knowledge.

Another point about use of facial recognition technology at public events relates to the need to be open, clear and specific about the intended policing outcomes from its use. The police being as open, precise and specific as possible about what they intend to use the technology for might be a mitigating factor and a way of beginning to facilitate a bit of trust. However, the issue is very complex.

Dr Bobak: I, will, if I might, add to that. As Christopher Lawless said, much also depends on how facial recognition technology is deployed. It might be done indiscriminately, which would involve surveying all the available faces, or there might be a more targeted search because, for example, the police are looking for 10 well-known pickpockets at a particular concert. Levels of public perception and trust in such targeted cases might differ from those in which, say, political marches are put under indiscriminate surveillance. A lot also comes down to transparency in how the software is used. Public information campaigns should be used to ensure that the public are aware of exactly how it is to be deployed.

James Kelly: The Scottish Parliament is currently considering a bill to establish a Scottish biometrics commissioner. Should use of live facial

recognition technology, and public confidence in such use, be high-priority issues for the commissioner?

Dr Bobak: Yes—absolutely.

Dr Purshouse: Yes. I will make a comparison with the situation in England and Wales in that regard. In the oversight framework, the UK Information Commissioner is responsible for giving opinions—she recently published an opinion assessing the operation of live facial recognition, which I recommend that the committee look at—and has enforcement powers. The UK Office of the Biometrics Commissioner's remit does not cover facial recognition technology; the role focuses solely on DNA and fingerprint data.

It would be good to bring facial recognition technology under the new Scottish biometrics commissioner's remit. I do not suggest that responsibility in that area should therefore be taken away from the Information Commissioner, who has an important role in looking at the data-protection implications of use of such technology. The advantage of extending the proposed biometrics commissioner's remit to include facial recognition is that the technology raises concerns that cover more than data protection. The data-protection concerns are very serious, but there are also broader human rights issues to do with bias and discrimination, the nature of our interactions with our public spaces and whether such technology is, on the whole, a social good. The biometrics commissioner could take a broader view of the impact and consequences of facial recognition technology.

Dr Lawless: With regard to the Scottish Biometrics Commissioner Bill, I note that some aspects of regulation of facial recognition could apply to a host of biometric data. It has been suggested that, for transparency, we should publish data on the performance of facial recognition technology: that could also apply to other forms of biometric data. The need for transparency around the procedure for establishing a match between an individual and a reference database could also apply in other areas.

We have watch lists for facial recognition. Similarly, most biometrics rely on comparing an individual piece of data with a collection of data, so the same principle perhaps needs to be considered with regard to the reasons for collecting some types of biometric data for comparison. As has been done with facial recognition, we could look at the need for advance warning to inform the public that biometric techniques are to be used in certain situations. We can learn from thinking about facial recognition a lot that could be applied to biometrics in the future.

Fulton MacGregor (Coatbridge and Chryston) (SNP): Good afternoon. Given that many of the technological developments will be driven by private companies, do you have any concerns about the possible blurring of boundaries between private companies and public bodies such as the police?

Dr Purshouse: Yes. I read with interest some of the committee's work on the Scottish Biometrics Commissioner Bill. It seems from the bill that the role of the commissioner is being established to look at biometric technologies as they are used for police purposes.

It is important to interpret that remit broadly because private companies, and even citizens, are increasingly using technologies that have biometric capabilities for what is ostensibly policing: crime prevention, detection, and personal or public safety. We saw an example of that in England and Wales, when facial recognition technology was used on the privately owned site at King's Cross, which is publicly accessible.

There is a blurring of private and publicly accessible space, and of private and public bodies that are using biometric surveillance technology. It is therefore important that terms such as "police purposes" are not interpreted too narrowly so that the commissioner can express a view and regulate those types of activities.

Fulton MacGregor: Do our other witnesses broadly agree?

Dr Lawless: Yes.

Dr Bobak: Yes.

Fulton MacGregor: Do you think that any legal framework should explicitly refer to those who have responsibility for capturing, storing and deleting images that are captured by live facial recognition?

Dr Bobak: In the public and private domain, or just in the public domain?

Fulton MacGregor: In the public domain.

Dr Bobak: My view is that that should certainly be regulated. It seems that Police Scotland already has an advanced approach to this and a sensible approach to the storing and deletion of images, but any such issues should be regulated.

Dr Purshouse: I think that it is important that the commissioner can cover both areas and the interplay between them, and that they can issue guidance as appropriate in the code of practice.

Fulton MacGregor: What about the more general question about private companies? You have answered the question about the blurring of boundaries between the private and public sectors, and I appreciate that answer, but what

about the financial interests of the private companies who are developing and selling the technology? Do you see any blurring of boundaries in that respect?

Dr Bobak: My view is that the way to mitigate that concern would be to employ independent academic experts in computer science to assess any potential software and to ensure that any public money is used in an appropriate way. When a call is made to purchase such software, the leading companies are private, so one can only go by what they provide as information. Someone who could independently verify any claims that they make would be extreme useful for law enforcement agencies.

Dr Lawless: I agree. Again, I refer to my earlier comments about using technology off the shelf. On the private use of biometrics, again, that is perhaps an area of concern that needs to be considered in relation to the scope of the Scottish Biometrics Commissioner Bill.

The Convener: I have a question for the panel—this might be unfair and I will understand if you are not in a position to comment. You might be familiar with some work that the sub-committee did on cyberkiosks. There seem to be a number of recurring themes about the capability of the equipment and such issues as collateral intrusion. Police Scotland responded positively to our report on the issue and has engaged with a stakeholder group and an implementation group. Is that the sort of approach that should be adopted in relation to the issue that we are discussing today?

Dr Lawless: Sorry, could you repeat the question?

The Convener: Do you think that Police Scotland's approach in not rolling out the cyberkiosk equipment prior to establishing a clear legal basis and prior to dealing with an implementation group and a stakeholder group that would include many of the organisations that responded to our request for information is a sound approach that should be taken in relation to the issue that we are discussing today?

Dr Lawless: I think so. I note that Police Scotland has halted the roll-out of cyberkiosks. I read the report on cyberkiosks and I was somewhat concerned about the level of communication with the police authorities with regard to the roll-out, because it seemed to me that some of the ethical concerns about cyberkiosks arose only after the move. However, reading the report, it seems that perhaps there was something of a learning process for all.

I was quite heartened to read some of the report's recommendations about emphasising a sense of caution and a need to communicate among stakeholders before any of that technology is rolled out and the need to think carefully about the ethical impacts. Maybe what happened around cyberkiosks has been something of a learning experience and has provided an opportunity to put some things right in terms of communication. The positive that has come out of it for me is that there is a recognition of the need for communication, for a certain amount of caution to be exercised and for the issues to be thought through before roll-out.

Dr Purshouse: There is definitely a recurring theme with the cyberkiosks and lots of these technologies. It seems like history repeats itself. I do not want to criticise the police and I do not think that there is any bad faith here. Part of the police's function is to prevent and detect crime as best they see fit, to use technologies as they become available and to experiment with them in order to do that. The police face pressures of budgets and the pressures that come when they have failed to exercise that function or have made mistakes.

Generally, the police approach that with good intentions. They want to have clear guidance and they want to use the technology within appropriate legal limits. It is the sub-committee's job and our job to set those standards. We must lead the way in thinking ahead to what technologies might be coming down the pipeline or are starting to emerge and take a proactive role in deciding what the appropriate democratic limits are and what the use of that technology in a human rights-compliant way might look like. There is a pattern here: the police use a technology and try to guess what the limits are, and then there is the back and forth of legal challenges, with regulation seeming to play catch-up. That is why I welcome you doing this work.

Dr Bobak: I agree. I guess people are in a difficult position, because technology develops very fast and some of it may or may not be useful for the police, bearing in mind their requirement to maximise their stretched resources. However, it is important that we engage in this dialogue, and this sub-committee represents a very good first step in that regard. In my opinion, a legal framework and clear guidance are paramount ahead of the rolling out of any live facial recognition software.

The Convener: That concludes our meeting. I thank the witnesses very much for their written and oral testimony, which was extremely helpful.

14:01

Meeting continued in private until 14:10.

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