



Justice and Home Affairs Committee

Corrected oral evidence: Live facial recognition

Tuesday 12 December 2023

10.30 am

[Watch the meeting](#)

Members present: Baroness Hamwee (The Chair); Lord Beith; Lord Blunkett; Baroness Chakrabarti; Lord Filkin; Baroness Henig; Lord McInnes of Kilwinning; Baroness Meacher; Baroness Prashar; Baroness Sanderson of Welton; Lord Sandhurst; Baroness Shackleton of Belgravia.

Evidence Session No. 1

Heard in Public

Questions 1 - 13

Witnesses

[\[\]](#) Ms Lindsey Chiswick, Director of Intelligence, Metropolitan Police; Paul Roberts, Head of Strategy, NEC Software Solutions; T/DCC Mark Travis, South Wales Police; Professor Karen Yeung, Interdisciplinary Professorial Fellow in Law, Ethics and Informatics, Birmingham Law School & School of Computer Science.

USE OF THE TRANSCRIPT

1. This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Examination of witnesses

Ms Lindsey Chiswick, Paul Roberts, T/DCC Mark Travis and Professor Karen Yeung.

Q1 The Chair: Good morning, everyone, and welcome to the House of Lords Justice and Home Affairs Select Committee. This is a short inquiry into live facial recognition and its use, following up work that the committee did a little while ago on artificial intelligence in the justice system, which turned out to be largely on policing. Live facial recognition, or LFR, turned out to be an important part of that, as I think we probably anticipated.

We are joined this morning by Professor Karen Yeung, who is online in Birmingham; Paul Roberts, head of strategy at NEC Software Solutions, which is a supplier of the live facial recognition software—I will revert to LFR soon; Deputy Chief Constable Mark Travis from South Wales Police, which uses the software; and Lindsey Chiswick, director of intelligence for the Metropolitan Police Service, which also uses the software.

We all have questions for you, and I am afraid we have more questions than time, which is almost inevitable in everything that we do. I will start by asking the two police forces if they can take us very quickly, using examples or making it live, as it were, through the process of determining when and where to deploy the technology. How do you determine which individuals make up the watchlist?

T/DCC Mark Travis: Thank you. Bore da pawb. Good morning, all. We have a very clear focus in terms of deployment of facial recognition to tackle the most serious crime and the most serious vulnerability. We have a benchmark by which we determine the necessity and proportionality of the use of the technology.

In answer to your question, as a live example, during summer this year three large-scale events took place at the Principality Stadium in Cardiff, which is a venue that holds in the region of 60,000 people and we used facial recognition technology to identify people who may be coming to that venue with the intent of committing crime. That could be serious crime such as terrorism, it could be crime against vulnerable people and against young girls and women such as people who may have an intent in relation to violence against women and girls, and then wider into acquisitive crimes—people who are wanted by the police for having committed crimes and people who may be involved in acquisitive crime.

We apply a serious threshold, and the decision to deploy the equipment is made by an officer of the rank of assistant chief constable or above—a senior officer in the service—to make sure that the benchmark of necessity and proportionality has been met.

The Chair: A senior officer takes the decision about deployment. I take it that it is in the stadium because that is where a large number of people will be congregating, so there is a bigger chance of you getting somebody who is on the watchlist. Does a live person take a decision about matching as well?

T/DCC Mark Travis: The decision to deploy is made by a senior officer. That is the authorisation to put the vehicle out on the ground. When we deploy on the ground, we have a person who is a specialist in the use of the equipment. We have 20 officers who are trained to use the equipment. It will be different for the Met, obviously. They determine whether a match has been made. That information is passed to an officer, and then the officer will engage with the member of the public in a very calm, relaxed way and have a simple conversation, much as we do with any engagement on the street with a member of the public, and determine whether or not we believe that we have a match for the right individual.

To put that in scale, we deployed our facial recognition system 14 times in the last year, and in that time we have identified a small number of people of interest and we had no false positives. So the accuracy of the system for us is small in number of deployments, small in intrusion and high quality in terms of its accuracy.

The Chair: Thank you. Ms Chiswick, do you want to add anything?

Ms Lindsey Chiswick: There is a slightly different way of deploying in the Met. It might be helpful if I talk you through what we did on Thursday evening when we deployed in Croydon. The deployment in Croydon was to tackle serious and violent crime. This year, Croydon has the highest murder rate. It has the highest number of knife crime-related offences. It has a blossoming night-time economy, and with that come problems such as violence against women and girls. That was what we call the intelligence case that sits behind the reason why we wanted to deploy there. It is very much linked to the intelligence case.

We then go to the watchlist. The watchlist is pulled together on the back of the intelligence case. On this occasion, on Thursday evening in Croydon, we were looking at crimes such as violence, other serious offences and people wanted on warrant. That included people wanted for violence against women and girls and for violent robbery. The watchlist is pulled together based not on an individual but on the crime types that I just talked about. It is then taken to approval from an authorising officer. In the Met, the authorising officer is superintendent level or above, and that matches other authorisations that we have on things like RIPA when it comes to directed surveillance authorisation, which is why we set it at that level.

Everything else is equal between South Wales and London in how we deploy the system. It is based on Authorised Professional Practice from the College of Policing. In the results from Thursday night, there were seven arrests: an individual wanted on suspicion of rape and burglary, someone wanted on recall to prison for robbery; failing to appear for a road traffic offence; criminal damage; possession of class A drugs; suspicion of fraud; and suspicion of drug supply and robbery. There were seven significant offences and people found who were wanted by the police who we would not otherwise have been able to find without the technology.

The Chair: Was that a specific occasion in Croydon or just because Croydon is a busy place?

Ms Lindsey Chiswick: It is a busy place. We are in the run-up to Christmas. There is a wider policing operation going on in Croydon at the moment, so policing resource was already deployed there. This was another tactic in a range of tactics that were being used in Croydon that afternoon and evening.

Q2 Baroness Chakrabarti: You will have noted that on Friday a decision came from Brussels that, within the EU, police and national security bodies will be banned from using real-time biometric data driven by AI in most circumstances without judicial authorisation, and even in exceptional circumstances, with a very high threshold of specific crime, there will have to be judicial authorisation within 24 hours. I suspect that that kind of legal development will have a bearing on the approach of the European Court of Human Rights in Strasbourg in due course, and indeed on policymakers and legislators in the UK.

In the meantime, my question is about the legality of what you are doing already. In your previous answers, you said, “We do this and we do that, and we set the threshold”, but I am interested in the source in even domestic law for your practice to comply with the Article 8 test of “in accordance with the law”. The Chair very kindly handed me a schematic and a slightly contorted diagram from, I think, the MPS website that refers to the Human Rights Act, the Equality Act, and the Data Protection Act, but, of course, they do not create police powers of any kind; they constrain them. What is the source of your democratic and legal justification for experimenting with and operating this kind of intrusive surveillance technology?

Ms Lindsey Chiswick: On the Met website, we have published our legal mandate. The legal mandate takes common law as the primary law. I think that is the diagram that you have in front of you. Underneath that, there is a complex patchwork of other laws that we pay attention to when we deploy live facial recognition. That is underpinned now by the authorised professional practice from the College of Policing. We are overseen by a number of bodies and commissioners who ensure that we are acting as we should according to that professional practice and according to the legal mandate and policy that we have published online on the Met website.

Baroness Chakrabarti: To be clear, there is no specific legislative authority for the deployment of this technology.

Ms Lindsey Chiswick: No, there is not, but the Bridges judgment and the Bridges appeal judgment found that common law was sufficient to be able to deploy that technology. That is what we are following and we are building on that the policy, the legal mandate and the standard operating procedures, which go into more detail about how we deploy.

The Chair: Ms Chiswick, I want to be neutral about this. I thought you might take the opportunity to refute the term “experimenting”. If you would like to, you might want to answer that.

T/DCC Mark Travis: We appreciate in policing that this is an emotive subject and we appreciate that people have very different views. I think “experimenting” is used, I

understand understand the context for why it is used. The Bridges case was really helpful for policing in the absence of the clarity that you refer to, and it made specific reference in relation to data retention, public awareness, the power to deploy, the gathering of information, and the impact on individual members of the public in terms of its use. It gave clear and further direction in relation to the management of equality. It has been very helpful for us to benchmark the way in which we have developed and deployed the equipment, and then for further scrutiny from internal ethics committees, our commissioner and the mayor, from London's perspective. There is significant oversight in using that benchmark to hold us to account in the deployment of the equipment.

Q3 **Baroness Shackleton of Belgravia:** To the police forces, how did your force reach a decision to procure LFR technology and then decide on the technology developed by NEC? When you are answering that question, please could you include how many other providers you considered? Why did you come to the conclusion that NEC should be the one that you went with?

T/DCC Mark Travis: The journey started in 2017 prior to the Champions League taking place in South Wales. Facial recognition was considered as a preventive measure to provide security to a major international event. A commercial exercise was run, led by a mixture of police officers and the procurement team, looking at a set of user requirements or a use case requirement for the procurement of facial recognition. The largest emphasis in the procurement decision was based on the quality of the solution. The procurement framework was run and delivered, and a preferred provider was selected. Four people were considered as part of that process. On the basis of the preferred provider meeting the threshold for the procurement framework, the contract was awarded.

It would be very fair to say that that is the start of an evolution. Whenever you engage with any form of contract or commercial engagement, the technology develops as the intelligence and the use case develops. It has been a journey that has seen us develop that relationship with our provider, and it has seen the same experience when the Met moved into this area of policing.

Baroness Shackleton of Belgravia: Did you consider the aspect of cybersecurity in relation to the very sensitive information that any procurer has and how effective that would be in a case where it was deployed against this material? Did the organisation come up tops in that test?

T/DCC Mark Travis: We have an internal specification in relation to the security standards of any provider that provides into policing: network security, information security, and the ethics of the organisation that we engage with. It would be fair to say that those standards have developed significantly in the last two to three years as a consequence of hostile state actors and things like that, so the position is constantly changing. I am not able to say—not because I cannot say it but because I do not know—whether it came top in every aspect of the procurement framework. I would need to take reference in relation to that, but it clearly benchmarked at a level that was satisfactory to meet our requirements.

Ms Lindsey Chiswick: It is very similar from a Met perspective. In 2016-17 we also started running trials and proofs of concept across a number of suppliers. We looked at five in total. Something that my colleague, Mark, did not mention and that both forces have been involved in when it comes to testing is the use of NIST. The NIST framework—the National Institute of Standards and Technology in the US—benchmarks different algorithms. One thing that we looked at when we were looking at those five suppliers is where the supplier comes on NIST, and NEC at the time was high. I think it is now even higher on both accuracy and bias. That was quite important.

The other thing we did was to hold some localised operational trials in Hendon with a range of different police officers from different backgrounds. Being a large force, the Met was able to draw on different people from within. We did our own tests of the technology. More recently, I am sure you are aware of the National Physical Laboratory testing that we did in the operational environment, which used much larger case studies.

Similarly, there was a huge interest in cybersecurity. Police forces have standards they must meet. The only thing I would add is that the system we use from NEC is a closed system, so that in the Met we are not plugging the system into other databases. It is a closed system that feeds itself.

Baroness Henig: Is it possible to estimate what percentage of cases are wrong? I was a bit alarmed when I read recently that there was some large-scale surveillance exercise done in one of the shopping centres in London, and that over half of the respondents who were said to be captured were not the right people. That may be right or it may be wrong, but it is what I happened to read. How accurate is this technology? What is the percentage where the pictures do not match at the end of the day? Maybe I will ask this about South Wales since you obviously have done a number of these things.

T/DCC Mark Travis: In the last year, we have reviewed 819,943 people. We have had zero errors.

Baroness Henig: It suggests that the technology is improving. That is in a sense what I am trying to get at. Is that reasonable to suggest?

Ms Lindsey Chiswick: That is what our evidence shows. I think we are on our third algorithm update from the provider at the moment, and certainly the number of false alerts has gone right down. The Met has not been as successful as South Wales when it comes to false alerts. Over 19 deployments and an awful lot of faces scanned, which have resulted in 26 significant arrests, we have had two false alerts. That is well below what the National Physical Laboratory put forward as the rate to expect, which was one in 6,000 with the watchlist sizes that we use. It is extraordinarily accurate, but I caution that that is one algorithm, and that is the algorithm that we are using at the moment from this provider. I do not know what your example in the shopping centre is, but it could well be another algorithm and another provider.

Baroness Henig: Yes, exactly.

Ms Lindsey Chiswick: There is a real mixture of good and bad out there, as you would expect with any technology.

The Chair: You both publish figures. Is that right? I have certainly seen figures from South Wales Police.

Ms Lindsey Chiswick: Yes.

The Chair: That is in the public domain.

T/DCC Mark Travis: Yes.

Q4 **Baroness Shackleton of Belgravia:** How did you gain confidence—you clearly have confidence—that NEC’s LFR technology works well? Is it under constant review? Obviously, you must have received advice before deciding to use that technology. Where did that advice come from?

Ms Lindsey Chiswick: To start with your first question, confidence in technology has grown over time. The NIST testing was a starting point. In policing, we have an ongoing duty to do what we can in terms of our public sector equality duty. It is an ongoing thing that we have to keep doing. A one-off NIST test is insufficient. We review after each deployment. We did our own testing. We continue to review after each deployment. Earlier this year, we were able to do the National Physical Laboratory testing, which showed us not only that the technology was accurate but how to operate the technology in a fair and equal way. When it comes to the operating threshold, we know how to operate the technology in a non-biased way. Now, after every deployment, we continue to review what has happened.

Baroness Shackleton of Belgravia: Do the contracts for the technology come up for review, and up to competition standards, so that other people can pitch for them, or is there a break? How does that work?

Ms Lindsey Chiswick: They will. I do not have the details to hand.

Baroness Shackleton of Belgravia: You are not overly dependent on these people for ever.

Ms Lindsey Chiswick: No, it is what we are using at the moment.

T/DCC Mark Travis: One of the benefits in the limited number of police forces that are using facial recognition is that the work between the forces means that our assessment is consistent. We are adopting the same approach in South Wales Police and the Metropolitan Police, which means that we can use each other’s data as a benchmark and a test. It is a limited environment. There are not many people we can ethically compare with. It is important that, against the College of Policing standards of professional practice and our own internal ethics committee direction and oversight, we seek to drive those standards and really push them to maintain the ethics of the equipment.

Ms Lindsey Chiswick: Both forces took advice from our ethics panels. In London, the Mayor's Office for Policing and Crime is linked to the London Policing Ethics Panel, and it provided five conditions for the ethical deployment of the technology, which we continue to abide by today. We took advice from MOPAC, the Information Commissioner's Office and the then Biometrics and Surveillance Camera Commissioner. We spoke to IPCO, the Investigatory Powers Commissioner's Office. However, because we are not using the technology covertly—we are talking about the overt use of the technology—the IP Act did not apply in the circumstances, although we talked to IPCO about the technology. We are currently talking to the Equality and Human Rights Commission. A whole range of people are able to provide advice about the various aspects of how we deploy the technology. There is ongoing engagement with a range of academics and civil society groups.

Baroness Shackleton of Belgravia: Thank you.

The Chair: It would be helpful, after the meeting, if you could let us know the answer to Baroness Shackleton's question about the length of the contracts. How long does the contract last? What break provisions are there? I am sure there are termination clauses as well before the term expires. I do not know, Mr Roberts, whether you have a standard contract. I suspect not.

Paul Roberts: It varies from customer to customer.

Q5 **Baroness Prashar:** Professor Yeung, has there been sufficient research and advice that is readily available to the police forces to enable them to make informed decisions?

Professor Karen Yeung: Perhaps I may be allowed to preface my comments by saying that what we have heard today is that the police forces are trying very hard to act responsibly in the use of this technology. In my criticisms which are about to come, there is no criticism of their motivations and their good intentions.

However, there is an important question to be asked when we evaluate technology about the claimed functional performance of software and whether it actually delivers the promised benefit in real-world settings.

The Chair: I am going to stop you for a second, Professor Yeung. I am having difficulty hearing, and I suspect others are as well. I am just looking at our technical people.

Baroness Prashar: Can you speak up a little, Professor?

Professor Karen Yeung: Yes, sure. Sorry, I will speak unnaturally loudly and hope that will be better. Is that a little bit better?

Baroness Prashar: Yes, that is much better.

The Chair: It is being suggested your mic might be a bit too high.

Professor Karen Yeung: Okay. How is that?

The Chair: Yes, that is better. Sorry, you will just have to keep your voice up. There are terrible acoustics in this room. They do not help you, either.

Professor Karen Yeung: No, it is fine. I want to focus on the question of operational effectiveness. Think about any time you thought about buying a new car or a new piece of kit. Will the system deliver the promised benefit in your specific contextual circumstances? I am told all sorts of amazing things about what a new piece of kit might do, but what I need to know is whether it will deliver in practice the promised benefits. That is where we need to keep in mind that there is a world of difference between accurate functional performance of matching software in a stable laboratory setting and in a real-world setting.

There is every reason to believe that the accuracy of the technology is getting better. I cannot deny that advances in computer science are travelling at a great pace. However, there is still a massive operational challenge in converting a match alert into the lawful apprehension of a person who is wanted for genuine reasons that match the test of legality. To do that, you have to have police officers on the ground capable of intervening in complex, dynamic settings to lawfully apprehend that person, bearing in mind that the mere fact that an alert is being generated does not in and of itself satisfy the common-law test of reasonable suspicion. When a police officer stops a person in the street, they do so on the basis of the voluntary co-operation of that person in producing identification. The mere fact of a facial recognition alert match is not enough, in my view, to satisfy the reasonable suspicion test.

In the latest data from the 2022 London Met usage, we are told that throughout the year 144,000 faces were scanned. That is a prima facie violation of the privacy of 144,000 people in public settings in London. They made eight arrests, none of which were for serious crimes. Many of them were for small drug offences and shoplifting. There is a divergence between the claims that they put only pictures of those wanted for serious crimes on the watchlist and the fact that in the Oxford Circus deployment alone there were 9,700 images on that watchlist. I would quite like to know how for each of those 9,700 images it was justified as lawful, necessary and proportionate to put those faces on the list.

Those are the questions where the police are not being given enough guidance, because the law is actually very difficult to apply. You need human rights expertise to apply it meaningfully. The police are going to struggle in making lawful and proportionate decisions in specific contexts. I do not think there is enough guidance or that it is clear enough. We need a legislative framework that makes that much more straightforward.

Baroness Prashar: Thank you for that. There are a lot of questions arising, but given the time I will not pursue them.

The Chair: I do not know. Our witnesses might like to respond to that.

T/DCC Mark Travis: Thank you. I am what is called a public order gold commander. I manage large-scale events. One of the things that I try to do is to achieve layers of prevention, layers of things to deter people coming to a location that people who might want to cause harm to other people. We both explained how we used the equipment slightly differently between the two forces. For example, we use the equipment at a large event with a large number of people where we are trying to create a safe environment. I can give you examples of people arrested for robbery, gang crime and very serious offences that meet the threshold of a serious offence as defined in law. It is inevitable that when people are wanted for offences they become involved in this type of operation. It does not mean that they do not justify being engaged with.

It is very clear that an image identified through facial recognition does not meet the threshold to arrest an individual. We stop and engage with the member of the public, as we do every day of the year when we stop a motorist and speak to them or when we stop a member of the public. We stop them and we talk to them. We try to identify whether they pose a risk to themselves because they might be a missing person, whether they pose a risk to somebody else because they might be a paedophile, or whether they are engaged in criminality.

I am personally of the view that the preventive and operational benefits of the system add value, save money and keep people safe. I also agree that it is a complex area of law and that the application of this system requires significant thought and proportionate use, which is why our deployment principles and the benchmark of deployment are set as high as they are in terms of authorisation and are as limited as they are in the number of deployments.

The Chair: You said earlier that your choice of venue—you gave the example of the stadium—was because of the numbers of people. Is that not slightly at odds with the point that you have just made about seeking to use the systems to find people who pose a danger to the public? I thought you said “in that situation”, but I might have read that in my own head.

T/DCC Mark Travis: To be clear, if we were at a pop concert where there were to be young people, we would be very concerned about people coming to that concert who may have an intent towards young people. We would use the system in a bid to prevent people coming in the first instance, to stop them coming because of the preventive measure, and, if they come, to identify them so that we can engage with them and make sure that people are safe. There is the issue of vulnerability. We have issues such as terrorism, which people think about here and are very much here, are they not? They are evident for you every day in your security at this site. We also use the equipment for missing people, young girls who are vulnerable and people who pose a risk to society who we otherwise would not be able to find. It is a very important part of our public safety strategy for major events.

Ms Lindsey Chiswick: I will respond to Professor Yeung on a couple of specific points, and then I want to talk through a little more broadly about what an officer

does when a match comes in. On the scanning of faces that Professor Yeung talked about, I want to make sure that everybody is on the same page and understands that that is fleeting and instantaneous. It is not kept. If you are not a match, your image is immediately and automatically destroyed. In the back of the van, the people watching those images coming past will see that it is pixelated, so they cannot even see the faces coming towards them.

The watchlists in London are large. There are a lot of wanted offenders in London that we are trying to find. Some will be local subsets. Let us take the example that Professor Yeung referred to, which I think was Oxford Street. In that example, some of the local subsets will be shoplifters, prolific shoplifting offenders who we have seen in the media that the shops are desperate to catch. There will also be some broader categories of murderers, rapists and those who fit into the really serious crime categories.

I will talk through how the technology works. If I am an officer, I look for people every day. In a morning briefing I might stand up and be shown pictures of 100 wanted people we are trying to look for. There is no way that as an officer I could remember those individual faces. All the technology does is up the chances of plucking that face out of a crowd. What comes after that at that point is normal policing and normal officer powers. All the officer will get is an alert. We train them every time we deploy what to look out for. They look at the alert and then make their own decision. Does that face look like the face of the wanted person? That is the human in the loop, which I am sure you have heard us talk about before, making the human decision. Then officer policing—normal policing—kicks in. They go and engage, as my colleague, Mark, said. They ask the person to identify themselves. If they are a wanted offender, that may lead to arrest.

The Chair: The distinction between the use of LFR and what you call normal policing is at that first stage. Does the scale of this go to proportionality and necessity?

Ms Lindsey Chiswick: When you say the scale of this—

The Chair: The scale of any given operation, because by definition it is bigger than a couple of officers who happen to be crossing Oxford Circus.

Ms Lindsey Chiswick: Regarding faces scanned, there are a lot of wanted people in London. I think there is a balance between security and privacy. For me, it is absolutely fair. When we look at public surveys, we see that between 60% and 80% of the public support law enforcement using the technology. That balance is right. I am quite happy for a fleeting, instantaneous glimpse of my face that is immediately destroyed if I am not on the watchlist—I am content for that to take place. Others may feel differently. The majority of the public in the surveys that there have been over the past three years are supportive. I am not sure whether you were talking about the number of officers involved in a deployment, but they are quite small.

Baroness Chakrabarti: I am interested in protesters who are not actually wanted for a criminal offence. I understand that South Wales Police has been lending

technology to other forces, and in particular you lent your kit to Northamptonshire for the Silverstone Formula 1 weekend, when the chief constable there said he was looking for protesters. Of the 790 names on his watchlist, only 234 were wanted for arrest, which leaves 556 on a watchlist who were not wanted for arrest for any crimes. I am just concerned about people on the watchlist who are potentially protesters, or others. You talked about victims and others who are not actually wanted for any crime.

T/DCC Mark Travis: I know the scenario that you are talking about. I was the person who authorised the deployment of the equipment to come out of South Wales. I will be very honest with you: the way it works is that we authorise the deployment of the equipment to another force. The force that it goes to then works through its own policy procedure to determine what it has sitting on its watchlist. The reason for that is that they understand their local threats. We have talked about differences in the threats between the Metropolitan Police and the South Wales Police. The local force makes a determination in relation to the necessity and the proportionality of the use of the equipment.

In the scenario that you are talking about, the specific issue related to a stated or intent or believed intent that people would try to access an environment that would put their lives or the lives of other people at risk. On that basis, that's why the force made the decision that it made. That is its decision to account for the use of that technology and its authority in terms of the actual deployment of that equipment.

I can tell you that from the South Wales perspective we have not used the equipment for protests. We do not intend to use it for protests as a routine matter. We do not see the necessity for that. There are far better technologies for gathering intelligence in relation to protests, from our perspective, than facial recognition. I do not rule out that, in the future, on the basis that there was a stated intent to cause a threat to the life of another, we would consider the use of the equipment. The watchlist for us in that scenario would be so narrow that it would be constrained to people who we believed had that stated intent. We do not use it for general protest activity, and it is not within the chief constable's direction as to how we will use it in the future.

Baroness Chakrabarti: Thank you. That is very frank and very helpful on the patchwork of totally differential criteria that are being adopted around the country by different police forces.

The Chair: I am sorry, Baroness Prashar. You were very self-disciplined, and we took advantage of that.

Q6 Lord Blunkett: I am not against the use of technology, but clearly we are talking here, as we have so far, about proportionality, the ethics and its practical nature. I wonder if you could say a word or two about training. I am referring to South Wales Police and the Met, but a manufacturer, Paul, and Professor Yeung might also have an interest.

How many people, and at what level, in South Wales and the Met are actually being trained not just in the practical use of the technology but in the broader issues that Lindsey referred to in terms of the ICO and the EHRC and the nature of what we are talking about, and not just at the approval level, whether it is DCC or superintendent level, but those operating and being responsible for how far they go at very local level?

Ms Lindsey Chiswick: We have seven officers who are trained in relation to the mobile units that we deploy. That is extensive training on facial matching, and they always deploy with the van on every deployment. Separately, when a deployment takes place, all the officers who will be out on the streets, making the interventions, having the engagement sessions, talking to and potentially arresting someone, always have a training input immediately prior to the deployment. That happens every time, even if they have been trained already, and it happened two weeks ago. We want to give them the most up-to-date knowledge and training and explain the watchlist based on the intelligence case for that specific deployment.

The training covers how the system works, what happens to the public data when there is a match and the fact that it is destroyed—the privacy-by-design features that I have already mentioned. We talk a lot about the human in the loop and that it is not the technology making the decision. We talk about the testing we have done, and the performance and accuracy of the system, including how we operate it to ensure that it is fair and equitable so that there is no bias. We talk also about unconscious bias. While we know how to operate the system in an unbiased way, the human operator who then takes the steps after the system has created the match needs to be aware of their unconscious bias.

Lord Blunkett: Who is doing the training?

Ms Lindsey Chiswick: One of the LFR team who has been through the significant additional training on how the system works.

Lord Blunkett: Who has trained the trainer?

Ms Lindsey Chiswick: Is that NEC?

Paul Roberts: It is, yes. As with all customers, we carry out two types of training—operational training and more technical training. As is common practice with suppliers of software to UK policing, we work on a train the trainer or master trainer model where we educate a number of people in the organisation. They then take the specific product knowledge that we give them, wrap it around with all the process and other issues that form part of the role of the person, and deliver that as a customised course locally, reflecting local force policies.

Lord Blunkett: I asked the question in the way I did because it is clear from the answers that we have already received that there is real fragmentation across the country in how people might perceive use of the technology and, therefore, the coherence and consistency of training between different force areas, including where you are reaching out, as in the Northamptonshire example given by Baroness

Chakrabarti. There is a fragmentation of training anyway, which I think was made worse by the previous Home Secretary. I am interested in where the external element of the training is coming from.

Ms Lindsey Chiswick: I am the director of intelligence in the Met and the SRO for the Met police use of this technology. I am also the National Police Chiefs' Council national lead for facial recognition. Through my national leadership role, we run a strategic board and bimonthly working groups where, as more forces gain an interest in the technology, we pool our advice. It is very much a joint board with South Wales Police, where we bring our advice and training, how to work through things like impact assessments and how we went about procuring and testing the technology.

You are right: we have recognised that previously there was a bit of a gap, and over the past 12 months or so we have really worked at bringing that national board together so that we can offer it as a font of knowledge for other forces that are interested in moving forwards with the technology.

Lord Blunkett: You are giving them advice, but that is not the same thing as training.

Ms Lindsey Chiswick: At the moment, there are no other forces, with the exception of the one in South Wales, using the technology.

T/DCC Mark Travis: To give you some confidence about consistency, accepting that you may want to challenge the way in which the training is constructed, the deployments that have taken place so far in terms of the use of the equipment on the ground so far have taken place in two forces, which have been the Metropolitan Police and South Wales Police. If we provide equipment to another force area, our trained staff go with it to make sure that the application and the use of the equipment is consistent wherever it is deployed, for want of a better phrase.

In the example that I was asked about in relation to the Grand Prix, South Wales Police operated the equipment. However, it operates the equipment with the watchlist provided by the home force. We are using our equipment with its intelligence. That means, Lord Blunkett, that there is consistency in the application of training and use between the two forces.

Lord Blunkett: Finally, I just want a one-word answer because this is a leading question. As this technology is rolled out and many more forces use it, is there not a need for both a national training programme and a standard that all can adhere to?

Ms Lindsey Chiswick: There is a standard through the introduction of the authorised professional practice at the College of Policing. I will take away your comments on training. As more forces come on board, it is very much an ambition that we would like to have. We are not quite there yet because, as my colleague said, it is only South Wales Police and the Met that have access to the technology, but, moving forwards, it is a really good idea that we will work on.

T/DCC Mark Travis: We welcome agile guidance that can move at the pace that technology and criminality move at.

The Chair: We have talked about Northamptonshire. I have seen somewhere that Essex Police is using, or going to use, the technology.

T/DCC Mark Travis: That is correct. Essex Police had a mutual aid operation where we provided the equipment, and its officers ran an operation in relation to threats around the night-time economy. They made, I believe, two arrests as part of that operation, they were for people who were wanted for offences that were more serious than the shoplifting analogy given previously.

The Chair: You have talked about training on the technology. We are starting, as you obviously have to start, a step or two back from that, with training in all the rights and privacy legislation that the country should be working under, and alertness to that and the advice available to officers who are making decisions. I was on a committee that went to an Air Force base where we were talked through procedures about decisions being made to use armed drones in the Middle East and having a lawyer available at the time of every operation. Do you have an equivalent?

Ms Lindsey Chiswick: All officers in the Met are required and obliged to do College of Policing training called “Information and You”, which takes you through your data protection obligations as a police officer. That is one example of a number of standard packages of training that all police officers must do. In individual, specific deployments, we take legal advice, as part of our regular catch-up when we are going to deploy the technology. We recognise the fact that it is still new and innovative. We are still building on our experience each time, and that legal advice is important.

T/DCC Mark Travis: It is a similar situation. All the people who can authorise deployment have been trained either as public order or firearms commanders, so they are familiar with the balance of Articles 2, 8, 10, 11 and 12. As part of our operational training for our staff, we focus our activity around the legislative use on a small group of people so that we are focused on how we apply it. The decisions that the officers have to make on the ground are theirs. We do not direct. It is their decision to make on the basis of necessity and proportionality. Traditional good policing skills—courtesy, patience, tolerance and understanding—are the things that help them get through and work out whether we need to make a decision.

I come back to the observation on volumes. We are talking about arresting five people in 2023 and identifying 10 people of concern in 2023 in total, so this is not an everyday tactic, with everyday use and everyday consequences.

Q7 **Baroness Meacher:** My question has largely been asked, but maybe I can ask Paul Roberts a quick question about “explainability”, by which I mean the ability to explain how a certain outcome was reached. How is explainability embedded into the LFR technology, if it is?

Paul Roberts: As background, we produce many systems that involve different forms of AI. We have been doing face recognition for a long time. We started our journey with that in 1989. Lindsey used the phrase “human in the loop”. In our design principles, we very much embody the human in the loop and ensure that, where we provide an alert or a notification, we are really drawing someone’s attention to look at something. We are not providing a direct call to action or a direct instruction. No decision has been made. We are simply bringing something to someone’s attention.

The way we do that in an LFR use case is through an alert, and that alert is when a member of the public has passed through the zone of recognition with an LFR system and their face bears a high degree of similarity to that of someone on one of the watchlists. Similarity is our measure of explainability, and it is a variable score. We have our threshold, which I think Lindsey mentioned, in terms of having been informed by the National Physical Laboratory testing on validating no bias.

There is a level where we are not generating lots of false alarms and where we are still generating alarms when serious offenders are going past and being recognised. We provide those alarms or alerts only when the threshold is met. When we provide alerts, there are two classes of officer we provide information to. The first is in the van. They have a larger screen. We display larger images of the face captured by the camera. Bear in mind that people are walking past the camera, lighting and angles change, and there are all sorts of technical challenges. We get the best face we can from what we have seen in the camera. We get the face from the watchlist and we provide them for human comparison of the two. We augment that with our similarity score. From that score, the officer knows whether it is just above the threshold, which is a maybe, or whether it is something really clear that the computer thinks with confidence is a strong similarity.

We display other information, such as the watchlist and whatever other things forces add, to the engagement officer outside the vehicle who may carry out the engagement with the public. They have all the same information, just in a smaller form factor. It is on a smartphone-type device. They can still see the faces and still have the similarity score as a mechanism of understanding. The face recognition similarity score is kind of accepted as the explainability basis for it.

Baroness Meacher: That is really interesting. Thank you very much. What information does the interface provide to empower operators to interpret and challenge the results provided? Do you feel that you prepare them to do that?

Paul Roberts: Human comparison is effectively the main element of that. In other face recognition systems, where perhaps we are looking at things after an incident has happened, we provide lots of tools to measure facial feature lengths and all those things. There is not really the time for that on a live facial recognition deployment. The period between a person passing the camera and then disappearing into the crowd is quite narrow, so in engaging with our customers there is no time window to provide more tooling than the human comparison.

Baroness Meacher: Thanks very much.

The Chair: I think the phrase “human in the loop” has passed its usefulness because it has become a bit of a mantra. One can deploy it, as it was deployed by a Home Secretary to this committee, without any detail of what is meant by it—that is personal and self-indulgent. Professor Yeung, do you want to comment on the training provisions?

Professor Karen Yeung: Yes, thank you. One of the real challenges is not necessarily in the match produced by the software, but the need, as Baroness Chakrabarti pointed out, for training in the legal requirements for populating a watchlist.

When an alert is generated and given the myriad categories of people that the evidence suggests and the kinds of justifications used to put someone’s face on the watchlist, there is all the difference in the world between someone who is wanted on a warrant for a serious crime and a person who has been identified as missing or vulnerable. Is an officer told the reasons why a person’s face has been placed on the watchlist? What is the explainability and justification for that specific face being on the watchlist? I would really like to know the answer to that question, and I have not been able to find it. I am not sure what training is provided on that very important piece.

The Chair: Let us see if we can hear it.

T/DCC Mark Travis: If the question is how we determine what is on the watchlist in category type—you gave the example of missing persons and vulnerable persons—we set criteria within the organisation that are agreed at senior officer level for each event, and then those categories will be drawn from our systems by classification to populate the watchlists. What you do not have is an individual officer looking at each individual person to say, “It’s this person, it’s that person”. We are looking at groups of people by category so that we can be confident about the reason why they have been brought on to the list.

A high-risk missing person by age or by vulnerability is something we can classify readily, and we draw that down under lawful necessity and proportionality in bringing that group of people into the watchlist. It will be the same in relation to counterterrorism suspects or people who have a history of sexual offending. We would use that group of people and that would be drawn together. The watchlist would be considered for each deployment to make sure that the categories were perceived to be necessary, but it is not individual identification of a person for each deployment.

Ms Lindsey Chiswick: It is absolutely the same in the Met. The only thing I will add to what Mark has just said is that there is quite a lot of information on the Met and South Wales Police websites about watchlist categories. There is information available for the public to see.

Professor Karen Yeung: There seems to be a bit of a mismatch between claims that the watchlist is populated only by those who are wanted for serious crimes. That is the official statement that the Met police have put out. Now we are being told that, in fact, the category of people is more variable. In a liberal democratic society, it is essential that the coercive power of the state is used to justify every single decision about an individual, and the fact that we are categorising people but we are not actually evaluating each specific person troubles me deeply.

Ms Lindsey Chiswick: I do not recall what particular statement that was, but I think I can explain it in terms of layering. Before we deploy the technology, we engage locally with the community. We engage with local shops, local businesses, retail or wherever we are going to deploy it. “Serious” for them is probably quite different from serious in another scenario. We can all accept that rape, robbery, armed robbery and murder are serious crimes, but if you are a retailer on Oxford Street suffering from prolific shoplifting and threatening behaviour to your shop staff, that is also serious criminality. It very much depends, in consultation with the local community and retail partners, what the make-up of the watchlist might be, and it may change according to where we are operating. The watchlist is destroyed after the operation, and a new watchlist will be created for the next operation, dependent on the intelligence case.

T/DCC Mark Travis: I am quite happy to take the challenge in relation to police trying to justify their position. I can speak from my position as a public order/public safety commander. I take a balanced view as to the impact or collateral intrusion we have on members of the public who come to an event where we have to keep them safe. I look at the tragic circumstances of events such as Manchester and other events where people have experienced horrendous injury as a consequence of individual people, a single person, carrying out a criminal act.

What I am trying to do is create a lawful, necessary and proportionate position of people being concerned that if they come to that event with criminal intent or hostility we will try to identify them and disrupt their activity. That is really clear for me. We cannot put the ring of steel that is around this building around our society. We would not want that. It would be too intrusive. What we do have to do is to create an environment where people can come, where mums and dads can come with their kids and feel that they are going to be safe when they go and watch a concert. That is a really difficult balance for us to strike in how we keep the public safe with the least intrusive measures.

The Chair: Let us continue on public perception with Baroness Sanderson.

Q8 Baroness Sanderson of Welton: Thank you, Chair, and thank you all for coming today. This is another question for the police forces. As we have said, the technology is sensitive and controversial, so the more that we can understand it the better. To that end, you have touched on this, Lindsey, but what methods do you use to communicate with the public about the use of the technology? How much information about its use do you share with members of the public? Is the

information easy for them to find?

For me, there is something as well, as Professor Yeung said, about the population of a watchlist. You say that, broadly, the public are in support of the technology, and I understand that if it is a national, general survey. But I live in Brixton where the community is already quite scarred by stop and search, and I am quite interested in what the community impact is in areas where you may be deploying this technology, such as Croydon, and what measures are in place to try to overcome that.

Ms Lindsey Chiswick: You are absolutely right. To refer to a Mayor's Office for Policing and Crime survey, we find that, as a broad catch, the public are in support of law enforcement use of LFR. When you drill down into specific community groups, that support starts to drop. That is something we are really interested in and have been doing quite a lot of work on.

There is loads of information out there on our website. However, I accept that the website is probably a bit difficult to read, and we need to do better on communications and find different ways of engaging with people. As part of that, we meet various independent advisory groups. We have been doing some work with young people and with different local community groups. If we were going to deploy in Brixton—we have not to date—and as we did with Croydon, before every deployment we would engage with the local community through the BCU to understand how people feel about the technology.

Quite often, what happens in that scenario is that the level of knowledge is quite low. When we arrive, there is a lot of reticence and negativity about it. By the end of the session, when we have been able to explain what we do and, probably most importantly, what we do not do and how we have managed to do work particularly on equality, minds change and people become supportive. Communications is a massive piece, and I feel there is more work to be done on that.

Baroness Sanderson of Welton: I want to refer to stop and search again. Wendy Williams in her HMIC report suggested that there should be scrutiny panels because it is a difficult power to use. Would you consider something like that in the use of this technology? There are different layers, are there not, as you have mentioned, in how you tell the public if they have been identified as a match and then human policing kicks in? If you have misidentified somebody, how do you stop them—it is the wrong person and they should not have been on the watchlist? I am a bit unclear about what happens in cases when somebody is on the watchlist and maybe should not have been and there is no reason for them to be, and how that works in terms of trust in the police.

Ms Lindsey Chiswick: It depends on the individual interaction. Officers are trained, as my colleague said, to act with empathy and the right, friendly interaction. Officers make stops and sometimes they stop the wrong person. If that happens, we find out through identification measures, whether a fingerprint or another check, and if they are not wanted and they are not on the watchlist they will be allowed to

go. The training is that that entire interaction should be commonplace in policing, along with a good level of engagement and empathy.

Baroness Sanderson of Welton: Forgive me because I should probably know this, but are the figures for that publicly available?

Ms Lindsey Chiswick: Yes.

Baroness Sanderson of Welton: Is it all publicly available?

Ms Lindsey Chiswick: For every deployment that the Met and South Wales do, we publish everything.

Baroness Sanderson of Welton: Would you consider scrutiny panels in a similar way as for stop and search? You put stuff on the website, but people do not necessarily look at the website.

Ms Lindsey Chiswick: I would not rule it out. Oversight is important. I want the oversight. I want to be overseen by a body with teeth so that I can prove and demonstrate how I am operating. There is lots of oversight that I ran through earlier, with various bodies and things.

Baroness Sanderson of Welton: Yes, it is more the public.

Ms Lindsey Chiswick: Yes, oversight is important, and, yes, if that is another way of doing it, potentially. The question for me would be whether we can streamline it and focus on the right questions.

T/DCC Mark Travis: It is very fair to challenge that there will be members of the community who do not trust policing. Our independent ethics committee and the oversight of police and crime commissioners and mayors is important in representing the voice of people who do not necessarily want to engage with us because they do not trust us. We have oversight in relation to stop and search in particular where use of force is used or contentious stop and search; we use members of the public to do independent advisory group scrutiny of what we do.

Your question provokes consideration around the equivalent of the ride-along scheme that we have with stop and search coming into the facial recognition world. The principle travels in a very similar scenario, where members of the community could actually come, observe, experience and then guide and support in relation to how we do it. It is worth our considering how we could bring more of that into this area.

Baroness Sanderson of Welton: Thank you.

The Chair: Can I remind our witnesses to speak into the mics? We have to deal with the acoustics of the room and the broadcasting and the recording.

Q9 **Lord Filkin:** I have a question first, if I could, to the two police forces, again about transparency. Can you confirm that you have completed the algorithmic

transparency recording standard collection for your use of LFR?

T/DCC Mark Travis: Where we are in relation to this is that six criteria are set. The documentation that we hold exceeds those criteria. We have engaged from the perspective of whether we meet that or not, and we are satisfied that we go beyond that. We meet that standard and further, and beyond.

Lord Filkin: Sorry, I may be being thick, but I did not understand whether that was a yes or a no.

T/DCC Mark Travis: We have assessed our use of facial recognition against the six criteria that are set within that standard. We have met those criteria and we exceed those criteria.

Lord Filkin: Does that mean that you have made a judgment that you do not need to register?

T/DCC Mark Travis: We have engaged with the body that has that oversight, and its view is that we have met the criteria. We have not registered at the moment.

Lord Filkin: I think I got it eventually.

The Chair: There is another question about registering, which comes before meeting the criteria.

Lord Filkin: That is what I was on about, Chair. If I heard the last sentence you said, you have not registered. Is that correct?

T/DCC Mark Travis: That is correct, yes.

The Chair: That is correct.

Ms Lindsey Chiswick: We have not registered either, but as my colleague said, looking at what is required, we meet those requirements. I am very happy to go away and register. Both forces meet the requirements. We have not registered. We can do so going forward.

Lord Filkin: I do not think any of us is claiming that registration on websites is the be-all and end-all, but there is an incongruity between what you said about the commitment to transparency in the public domain and the fact that you have not registered.

The Chair: If I could add to that while you are thinking about the answer, the Government made a considerable point to us about the possibility of registering, and expecting registration, when we asked questions about public understanding and knowledge of what is going on in our society, to put it very broadly, and when we talked about regulation and asked why the AI systems are not regulated.

T/DCC Mark Travis: We are happy to register. The decision around professional practice is not our decision. We will make a recommendation that the registration is included within professional practice. We cannot make that decision.

The Chair: As a professional lead, Ms Chiswick, you could take that back. I am thinking back to the evidence that we had a couple of years ago. I know that life has moved on a little, but it has not moved on to regulation, so I think we would still hear the same point being made.

Ms Lindsey Chiswick: I will commit to take that away to the national strategic board, which sits this Thursday, so it is perfect timing. We will move forward with that and, as my colleague says, get it attached to the authorised professional practice so that people know that there is an expectation to fill it out.

Lord Filkin: Chair, as you have asked my question so well for me, can I deal with a wider question, briefly? It is obvious that technology moves significantly faster than regulation. My question is to Professor Karen Yeung. What is coming down the line next that policymakers and regulators should think about, otherwise we will be well behind the game?

Let me give you an example, to try to make my point. If I have understood it correctly, LFR is essentially site-specific at this point. I would expect that the technology would make it perfectly possible to connect multiple cameras to a very large database and, therefore, for example, to search across London almost simultaneously for suspects. Karen, do you think that is possible, or will it be possible soon, and what does it imply for the need for regulation and legality?

Professor Karen Yeung: That is a very good question. Technically, it is already possible in so far as the camera infrastructure is already in place, and you just need a very high-quality internet connection to do it. This is where the analogy of “I only saw you naked very briefly” does not work. What we are talking about, as the former Biometrics Commissioner said, is moving from the equivalent of line fishing to deep ocean trawling. This is surveillance at scale remotely that is possible across an entire nation in real time. I have a former researcher who is from China. He says that you cannot walk anywhere in public or even into a shop without being identified as a specific individual. It is a very powerful technology. The capacity to scale up is readily malleable once the infrastructure is in place. You can see the attractions for control within that, and that is why I think that we need—[Inaudible.]¹

Lord Filkin: That is exactly what I feared would be the answer. There could be theoretical benefits to that. Could I get the response of the two police forces as to what they think is required for an effective system of transparency and state regulation—because this will be with us within a year or so—obviously in terms of what is possible?

Ms Lindsey Chiswick: All this is possible, and more, probably. But, while there is that dystopian, quite frightening future, if I can bring us back to the here and now, we need to go back to the law and how it operates and how we work on necessity and

¹ The witness has clarified that her point was as follows: “You can see the attractions for control within that, and that is why I think that we need to have a specific legislative regime that provides clear and effective safeguards to ensure adherence to respect for democratic rights and freedoms and the rule of law.”

proportionality. That is really important. That is the thing that we will keep coming back to. It is the necessity and proportionality of operating in that area at that time with an intelligence case behind it, and the means of policing to respond.

To take the example Professor Yeung was talking about, which was using all our existing cameras, we should bear in mind that they are quite high, so the angle will not be quite right to catch a face. Even if it was, and even if we could do all that, there is necessity and proportionality in doing that, and you would also need an officer on hand to react and respond to the match. It simply does not work as a set-up. If we come back to the law and, underpinning the law, the authorised professional practice, underpinning our activities in policing is oversight and the importance of that, which we have talked about.

Lord Filkin: That is very optimistic. Let me not interrupt. Let me hear from South Wales first.

T/DCC Mark Travis: In the case that we articulated to you, one thing that is a benefit is that the public can see that facial recognition operations are in progress, because they are overt. There is signage; there is a big white van and the van has signage on it saying what it is. We engage on our website. We tell people. If policing moves to a position where it is not overt for the public, that is when we need to think very seriously about our relationship with the public in terms of transparency and what that might mean. It is a big step to go from facial recognition mobilised in a vehicle to facial recognition mobilised on infrastructure. That does not necessarily mean that it might not be the right thing to do, or the right thing to do for particular events, but there would need to be clear direction about how it should be delivered, through really tight professional practice, to make sure that it was governed and managed appropriately.

The difference with what we were talking about there as well, on the back of the point that Lindsey made before, is that at the moment facial recognition is a closed system. The minute that you start to integrate that into camera systems, you start to look at network solutions, and that becomes more challenging, so there are wider considerations, beyond the moral and civil liberties issues, in information security and how that becomes infinitely more complex.

Lord Filkin: Yes indeed. What you have said and what we have opened there raises a pretty big issue that requires significant parliamentary scrutiny and consideration. The few words that were said by Lindsey at the end, and more, are also important. We need to have sight of what looks as if it is coming, rather than reacting to what happened two years or so ago. We need to open up the extremely difficult balance of crime and security enforcement against the civil liberties that this poses. This is not a job that individual police forces can do, so it requires a wider process. Thank you, though, for that input.

Q10 Lord McInnes of Kilwinning: My question is to Professor Yeung. Clearly, transparency of algorithms is a hot topic in many walks of life, not least LFR. I would be interested in your view as to how the competing concerns of public safety and

commercial sensitivity for suppliers of algorithms can be balanced against the public transparency needs of people understanding the algorithms behind LFR when put into practice.

Professor Karen Yeung: Thank you for your question. I will start with the public transparency issue. We need to think about it in terms of community transparency in the way the system is used and administered and to have confidence that it is being administered in accordance with legal requirements. Then we have local explainability or contestability for an individual who is dragged into the net, being asked to respond to an alert, for example, or any other application from the use of biometrics.

As to global transparency, there is a legitimate concern that, if there is too much transparency, the system might be gamed. Persons who are genuinely of interest because all they want to pursue is crime might then avoid the area. There is a legitimate concern about gaming prior to deployment in a specific context, but that does not affect the need for ex post transparency and accountability. I do not really see why there cannot be very public information that justifies use in a particular case, with a very clear statement of the categories, the number of people whose faces were on there, and why. I think there is still a possibility for meaningful transparency ex post that gets around the genuine gaming concern, so I think that it can be handled in that way. I still have concerns about local justifications and the appropriateness of explaining to a person why their face was on the watchlist. I am still troubled by that. I do not feel entirely satisfied.

On commercial confidentiality, there is a tension with the legitimate interests in commercial software producers such as NEC wanting to keep secret the inner workings of the algorithmic system. We know that in the Bridges case there was no exposure of the underlying training datasets to evaluate the equality implications of that software. For my own view, I think the way that that can be resolved is through using the general approach of covert security, where you have an independent agency that scrutinises, without making it public, and has integrity so that there can be evaluation and testing under the hood which does not infringe commercial confidentiality. There is a way of mediating those tensions through appropriate institutional safeguards and settings, but they are not currently in place.

Lord McInnes of Kilwinning: To follow up on that very quickly, can I ask the three panellists in the room whether, in principle, they would have an issue with some independent body having full access to transparency after the fact of any LFR programme? Paul, might we begin with you?

Paul Roberts: From a supply point of view, I guess the nearest analogy is the Colonel's secret blend of herbs and spices in KFC. We invest vast sums of money in getting our algorithms to the point of highest accuracy and no bias, and training data is fundamental to that in the mix of images that we legitimately source and utilise in building our models. Inherently and organisationally, we have a nervousness around that position. I am happy to take it away and discuss internally

the options that Karen presented around independent scrutiny. We certainly understand the tension between the two.

I was the witness in *South Wales v Bridges*, so I was able to do certain things. For example, to satisfy myself with our algorithms produced in Japan, I looked at the laboratories in Japan and I was able to access certain data that allowed me to say under oath that I understood that they were representative datasets that seemed appropriate to the needs. It is not quite independent, but it is a level of access that would not normally be there, so I am happy to take that away and look at how we might be able to come up with a solution for that.

Lord McInnes of Kilwinning: Lindsey and Mark, do you think that this is a way forward?

Ms Lindsey Chiswick: We did what we could, given what Paul has said, to meet our public sector equality duties through the independent testing that we did with the National Physical Laboratory.

T/DCC Mark Travis: I do not have an objection to oversight and scrutiny, or support guidance, as long as it is well informed and cohesive with the other guidance and scrutiny that we have been given, so that we are working to a framework that is clear in its direction and they are not at odds with each other, or not in conflict. If we take advice and guidance, it has to be consistent so that we can work with it, understand it and use it.

Paul Roberts: May I add one small point? The focus in these things is often on the input to the model, when in many cases it should be the output. It is very hard to assess the input to a model. It is really the output from the model, which the NPL tests and the NIST tests do. Hopefully, that gives people confidence, in the range of scenarios, that accuracy is maintained across genders, races and all the different attributes. We are happy to look at the input part of the model, but the output part is very public already.

The Chair: Oversight, scrutiny and accountability.

Q11 **Lord Beith:** What do we know about the frequency or number of cases taken to police complaints commissioners or the deputy mayor? Do we have any experience of that?

Ms Lindsey Chiswick: I am not aware of any formal complaints about the Met's use of the technology. I am on a strategic board in the Met once a month, and a member of MOPAC sits on that board. That is where we review each deployment, and we do larger reviews from time to time. I know some boroughs do not want to use it and have talked about not wanting to be part of it; they are boroughs that I would really like to engage with, if we are not already engaging with them, to talk them through the technology and how it works, going back to the earlier point about levels of understanding. I am not aware of any formal complaints to MOPAC.

Lord Beith: I am thinking of the person who did not want to spend his afternoon

being engaged with by police officers but hoped to watch the football match or attend the January sales, and does not want to be identified to those around him as someone the police are interested in.

T/DCC Mark Travis: We advertise on the police and crime commissioner's website and on our vehicles how people can access and engage if they want to make a complaint. We are almost inviting it, if I can be quite honest, in how we present that information to the public. We have not had a single complaint. Some people might say that is because people do not trust our complaints system, and that is a fair observation. There are people who do not trust our complaints system, but the route and the opportunities are there, which is why I think we need to go away and explore the proposal in relation to the oversight visibility ride-along type of approach that was talked about previously, where independent members of the community can observe and see what is going on.

When we talk about engaging somebody, if that person is not who we are looking for—bear in mind we are talking about literally a couple of false positives across the two forces, and none in South Wales—we are not taking their time in an unnecessary manner. When we engage with people, it is generally quite a quick interaction, and if it is not a threat to the event they will be able to go on their way. If they are wanted on a warrant or they are going to be arrested, they will not get to the football match; they will go into custody. Ultimately, we would say that that was necessary and proportionate. The intrusion from this in time is very limited, and it would not stop people who are legitimately going about their business getting to that event.

Lord Beith: I have a wider question. What protection do we have against a hostile state acquiring access to these systems and using them in their pursuit of dissidents, for example?

Ms Lindsey Chiswick: We talked earlier about cyber protection and its being operated to a standard across policing to ensure that it is safe. The system is a closed system. It is not linked to other policing networks, which helps as well; it makes that level of security easier to complete.

With regard to the system itself, the watchlist is created for the intelligence case. It is uploaded on to the system 24 hours before and is deleted immediately afterwards because we do not need it any more; there is no policing purpose in retaining it. Throughout the time it is on the system, there are levels of authority about who has access to it. It would be quite difficult to access, although we know that hostile states have lots of tools in their capability, so they probably could if they really wanted to. I guess my question would be: why would they want to access a list of our wanted offenders across London?

Lord Beith: If they could identify dissidents would be the reason, I think.

Ms Lindsey Chiswick: Unless a dissident was wanted for a crime that fell into our watchlist, they would not be on the watchlist in the first place.

Baroness Chakrabarti: That is not true, is it, because of the example in Northamptonshire, where a number of people were on there who were not wanted for a crime?

Ms Lindsey Chiswick: Wanted criminals are one aspect of a watchlist. We have already talked a little about victims and witnesses. We do not have a watchlist category for dissidents. We cannot rule out a dissident getting on a watchlist, but off the top of my head I cannot think of an example of why and when.

Baroness Shackleton of Belgravia: I think the answer to the question of what they would want it for is that they may want it to blackmail the police for money, because they do not know what they are going to use it for. People hack into systems, not because they necessarily want the information. That information is valuable to the police and would be valuable as a tool to extract money.

Ms Lindsey Chiswick: Taking a step back, if they hacked into the system, and if there was a picture of a dissident on the system, what would they have access to? It is a closed system and the watchlists are retained for the period of the 24 hours' deployment, so they could access a photo of the dissident, which they may already have. I am not really sure what else they would have access to.

T/DCC Mark Travis: There would be no identifier as to address, contact details and things like that. None of that kind of private information is held in the system.

Ms Lindsey Chiswick: It is just a name and a picture.

T/DCC Mark Travis: It is an identification.

Baroness Shackleton of Belgravia: It is just one picture, but there could be access to a system with a whole lot of pictures in it, and they could then say, "These are the people the police are interested in", which you might not want to disclose to the public generally.

Ms Lindsey Chiswick: That comes back to the fact that the watchlist created for the deployment is kept for only 24 hours and is specific to that case. Even if they accessed it, they would not have access to the whole system of images that the police have as part of their custody image database.

Lord Beith: A good question, which I will not go into, is that a person could, effectively, be part of a watchlist without being visibly part of it, but that is for another day and another witness.

The Chair: You have been using the word "dissident", but if I substitute the word "protester", is the answer the same?

T/DCC Mark Travis: Yes, the answer is the same. The concern that we would have as professional police colleagues would not be the accessing of this data but the accessing of wider police data, the police national database, which is the system that holds the breadth of information that allows you to understand the picture of

an individual, where they are, who they are and their associates. Accessing something like that would be fundamental in terms of those risks, which is why we have such significant safeguards for those elements. What we are talking about here—I am not saying that it is not significant to the individual—is a small snapshot of that data, which is divorced from what we call their nominal data. For example, a hostile state knowing who an individual was would be able to identify a photo and match the photo, but if you did not know that, because you were not a hostile state, it would have no bearing or no benefit in an intelligence picture for anybody.

The Chair: Professor Yeung, do you want to come in on all this? I wonder whether there are any useful international comparators. I say “useful” because there are different legal systems. If they are not comparable, one does not necessarily have a read-across.

Professor Karen Yeung: It is useful to locate the discussion that we are having in this room within the larger international context. I am sure that everyone is familiar with objections to the use of this technology by civil society organisations. For example, in Europe alone, it has been banned entirely in Luxembourg and Belgium. The AI Act will basically ban it in Europe once it is enacted, subject to very limited law enforcement exception, requiring higher judicial authorisation and only for specific serious crimes. It is much more limited than the way it is currently being used in the UK. It is used everywhere in China and it is the norm. There is a question about whether that is the kind of political community that we wish to be, and that is where we need to be mindful of the fact that we are an outlier as a democratic state in the pace at which we are embracing these technologies.

The Chair: We have mentioned ethics committees, and one could say that we should have started with questions about ethics.

Q12 Baroness Henig: This has been a really interesting session, not just with the specific focus questions but raising some very broad issues that we clearly cannot deal with today. The more it has gone on, the more I realise how important an ethics focus will be. Given the lack of an agreed legal foundation, ethics becomes, in a way, the place where a lot of these issues can be raised. Perhaps I could ask Karen about the use of ethics committees. Is there a common framework for them? Do they just spring up ad hoc? How do they operate? Can you tell us something about them?

Professor Karen Yeung: That is a really good question, although I do not have specific expertise. A study was done and reported in August this year, for which I can give you the reference, into the 43 policing localities and, it turns out, based on the survey, that a substantial majority of police forces have an ethics committee. There is no generalised framework or structure. They were largely divided into two types. The first type used their ethics committee largely as a kind of expert panel for ad hoc ethical dilemmas. The other type incorporated ethics committees into their internal governance structure and they incorporated a whole range of types of reporting, which included human resources questions, for example. There is quite a diversity of ways in which such committees are set up. They are increasingly used.

There is no obligation to use them, and, of course, the advice from an ethics committee is not binding.

Baroness Henig: I will defer to Guy, because I know that we are short of time and he will take this forward.

Q13 Lord Sandhurst: I have some specific questions that require yes or no answers. They are first directed to Deputy Chief Constable Travis. The South Wales Police ethics committee is an independent committee. Do we not need a national data ethics model on a statutory basis, with national guidance?

T/DCC Mark Travis: I want to answer your question accurately, so I need to use more than one word; I apologise. We have an internal and external ethics committee who support us. The complexity of this area of business, which has been highlighted today and has just been discussed, would be beneficial if there were a form of central reference that had subject matter expertise in a complex area. Whether that is statutory, or how that is formed, is a recommendation or decision for other people, but would we want to have that facility and that support to make effective decisions? I think that would be of benefit to us.

Lord Sandhurst: I did not realise that you had two committees. Can you explain the difference?

T/DCC Mark Travis: The internal ethics committee consists of people from our own organisations who make observations and recommendations about challenging questions. The external ethics committee is made up of professionals, predominantly with a professional educational background, who form a committee and who then, if necessary, they can go directly to the chief constable with any form of challenge.

Lord Sandhurst: They are dealing with what I call the policy rather than the day-to-day issues.

T/DCC Mark Travis: They deal with everything, in the way that Professor Yeung described, from policy and procedure through to staffing issues, issues around equality, all sorts of things. They have looked at the issue of—

Lord Sandhurst: Their decisions are minuted. Am I correct?

T/DCC Mark Travis: They are minuted and they are publicly shared.

Lord Sandhurst: If the force decides not to follow a recommendation, is that minuted or a matter of public record?

T/DCC Mark Travis: Yes.

Lord Sandhurst: Good. Can I turn to the Metropolitan Police? Who appoints the members of your ethics committee?

Ms Lindsey Chiswick: It is the London Policing Ethics Panel (LPEP), and I believe that it is appointed by the Mayor's Office for Policing and Crime.

Lord Sandhurst: Does it publish minutes?

Ms Lindsey Chiswick: Yes, it does, on the MOPAC website. It commissioned a report on the Met's use of live facial recognition, which is also published, including the response by the Met about how it is going to meet the five conditions for the ethical deployment of the technology. That is all available on the website.

Lord Sandhurst: Presumably, the Metropolitan Police is not obliged to follow a recommendation—or is it?

Ms Lindsey Chiswick: It is not statutory, but why would we not follow five very good and sensible recommendations for the ethical deployment of the kit? I think, from the MOPAC oversight perspective, when it comes to new and innovative technology—or sensitive processing, as it is in this case—it would check and oversee that we are responding to the LPEP recommendations.

Lord Sandhurst: Is it a matter of public record if there is non-following by the police?

Ms Lindsey Chiswick: We have written to show how we would follow it. I cannot imagine a circumstance where we would not.

Lord Sandhurst: Well, it has not happened yet.

Ms Lindsey Chiswick: We could write to them and tell them that we would not.

Lord Sandhurst: All right. Would you also agree that it would be helpful to have national guidance, possibly on a statutory basis?

Ms Lindsey Chiswick: I think that there is some work across policing—it is not my area of expertise—to bring together a national data ethics board. That would be very useful. Other places that we go to are the CDEI—the Centre for Data Ethics and Innovation. The Alan Turing Institute has been really useful with help and advice on data ethics. There is some national work, but I am not sure how advanced it is.

The Chair: We have slightly overrun but let us see whether any members have further short questions, presuming on your ability to stay for another two minutes. For some members, this is something of a revelation. It certainly was to those of us who were on the committee a couple of years ago, doing this work. As Baroness Henig said, the more questions you ask, the more questions you want to ask. Is there anything that the witnesses would like to leave with us that they feel we have not properly covered or that they would like us to amplify?

T/DCC Mark Travis: The last question was in relation to oversight and scrutiny. The police and crime commissioner structure in south Wales and the mayor's structure in the Metropolitan Police are very keen to get this right, on the back of the complexity that exists around the position. We are very keen, as police officers, to

get it right, and you have suggested a number of things today that we will take away and consider. We are very open to suggestions and recommendations on how we move this area forward. We recognise the significant impact of the use of the technology, which is why we are so determined to manage it in the most effective way we can. Thank you for your time.

Professor Karen Yeung: I have a few brief comments. One of them is the importance of recognising that, because the technology operates at scale, it has the capacity to change the default political and constitutional culture and environment in which we move about lawfully in public spaces, and that, I think, is easily lost in these discussions. I just want to remind the committee of that.

The second piece that I want to emphasise is that, even though the claim is that the intervention is minimal, we need to remember that there is a really stigmatising effect in being singled out by a police officer as you are going about your lawful business in public. As a non-white woman, I am very conscious of how that can have a differential impact as I move about the world, particularly in airports, for example, in a very troubling way. I want to remind the committee of the reality of that experience.

The Chair: That is the point that Lord Beith was making, although I am not sure whether I would catch you at the January sales or a football match, Lord Beith.

To all our witnesses, thank you very much. This is a very short inquiry, too short for the subject, but it is the best that we can do in the time we have available before the membership of the committee changes. We wanted to use this opportunity to pursue points that we identified a couple of years ago, but knowing that life and technology move on, it is quite hard to keep up and be on top of it. Thank you all very much indeed.