HOUSES OF PARLIAMENT

Joint Committee on Human Rights

Oral evidence: Biometrics and Surveillance Camera Commissioner, HC 1128

Wednesday 22 February 2023
3 pm

Watch the meeting

Members present: Joanna Cherry MP (Chair); Lord Alton of Liverpool; Lord Dholakia; Dr Caroline Johnson MP; Baroness Kennedy of The Shaws; Baroness Lawrence of Clarendon; Baroness Meyer; Bell Ribeiro-Addy MP; David Simmonds MP.

Questions 1 - 18

Witness

I: Professor Fraser Sampson, Biometrics and Surveillance Camera Commissioner.

Examination of witness

Professor Fraser Sampson.

Q1 **Chair:** Welcome to today's meeting of the Joint Committee on Human Rights. We are a cross-party committee of both the Commons and the Lords. Today we are hearing from the Biometrics and Surveillance Camera Commissioner, Professor Fraser Sampson. The purpose of our session today is to look at the role and work of the Biometrics and Surveillance Camera Commissioner, and the human rights issues raised by the use and regulation of biometric data, the use of surveillance and the use of artificial intelligence technologies such as live facial recognition by the police.

Professor Fraser Sampson has over 40 years' experience working in the criminal justice sector. He served as a police officer before becoming a solicitor specialising in policing law, conduct and governance. On 1 March 2021, he was appointed by the then Home Secretary as the Biometrics and Surveillance Camera Commissioner. His tenure was due to end next week on 28 February. However, we are very glad to say that, on 9 February, the Home Secretary reappointed him to continue in his role. We are delighted to have him with us today.

Could I ask a couple of scene-setting questions, Professor Sampson? I wanted to ask you, before we do anything else, to confirm what biometrics are.

Professor Fraser Sampson: Thank you very much for that introduction and for the invitation to appear before you. The reason for this smile is that biometrics depend who you ask. If you were to ask the Government, there would be a sub-question: "In what context?" In the context of policing, biometrics are confined to fingerprints and DNA profiles and samples. If you ask in relation to schools, there is a wider definition even for England and Wales, and Scotland has a much more descriptive definition under its legislation.

My own response in relation to the practicalities—what the person in the street reasonably expects when you ask them that question—is that it is any unique manifestation of your membership of our species that can be accurately measured, recorded and compared with other records for congruence with a predetermined level of points.

Chair: So it would include fingerprints, in general terms, DNA and facial recognition technology.

Professor Fraser Sampson: Yes.

Chair: Does it not now also include things such as gait and emotion?

Professor Fraser Sampson: I believe so. My office attended a meeting recently at which there was a question as to whether DNA ought even to fall within the definition. There is a drift towards excluding lots of things rather than including them, but the expectation of the police, local

authorities and the people I work with on a daily basis is that, if you can measure it and it is part of a human's behaviour—gait, as you say, ear prints and palmprints—it is a biometric. Voice is a really obvious one that can be measured very reliably and compared with other records, and it has a degree of permanence, so it does not change particularly over time and is individual to that person.

Chair: Most of us are familiar with using a fingerprint to unlock smartphone technology. My banking app requires me to blink my eyes before I pay my bills. Would that be covered by biometrics?

Professor Fraser Sampson: Yes.

Q2 **Chair:** This committee obviously focuses on human rights. I would like you to describe for us, before we get into any detail, the most pressing human rights issues you have encountered in your work and how you have approached them.

Professor Fraser Sampson: They probably point in two directions. The ones that get the most attention are the ones that have been covered by a lot of direct legislation, debates and coverage in news outlets, which will demonstrate the increasingly, and in some cases novelly, intrusive capability of new technology. There are more and more ways of measuring your presence on earth and your movements around it, and then comparing them.

The ability to measure that, and the proliferation of tools that measure it, whether you want them to or not, means that there is a significant move towards considering the impact on areas of human rights; in particular, various articles from the convention are under serious consideration when it comes to biometric surveillance.

The other one, which gets less attention, is the positive obligation on the state and the police, such as you find under Article 3, to use biometric and surveillance technology to prevent citizens suffering inhumane or degrading treatment along the lines of cases that we are familiar with. The more we can do that, and the closer to police investigations the means to do that get, the more legitimate expectation there will be that the police will at least explain why they did not use that in an event where they could have protected someone and did not.

Chair: That is the positive obligation. You also mentioned the intrusiveness, which would engage the right to private and family life, under Article 8, and the right to dignity. What other articles of the ECHR might be engaged by the use of biometric or surveillance technology?

Professor Fraser Sampson: A great many of the others would be. Examples include things categorised traditionally as having a chilling effect, which might prevent people exercising their right to meet in public or the right to freedom of speech if they think they are being recorded by street surveillance cameras.

There are areas where I deal with national security determinations relating to freedom of movement internationally, and freedom of religion and thought, because assumptions may be being made in forming an intelligence picture on individuals. Plainly, there are Article 14 issues of discrimination, bias and adverse impacts on any particular individual or group of individuals, engaging the public sector equality duty for the areas that I cover.

Then there are more subtle, but equally important, areas, which I have spoken about quite widely in public, such as engagement with providers of the technology that is being used to measure these increasing manifestations of our individuality.

Chair: Can I clarify a couple of things before we get into exploring in detail the implications of some of the rights that you have mentioned? Your remit covers England and Wales only. That is correct, is it not?

Professor Fraser Sampson: I have two statutory hats on. The Biometrics Commissioner is UK-wide. The Surveillance Camera Commissioner is England and Wales.

Chair: I do not know whether you feel able to comment on this, but it is quite topical. There was a very interesting interview with Tony Blair and William Hague on the radio this morning about their report published today on using technology to transform the UK's economy and society with these big ideas. In response to a question about their recommendation for a digital ID on mobile phones and people's fears of the implications of that—it was described as all that can and does go wrong in the digital world, and the mistakes and losses made—the former Prime Minister Tony Blair expressed his confidence that modern biometric technology can overcome many of the problems with digital ID.

Do you agree with them? If you want to speak not with your commissioner's hat on, but from your experience as a police officer or a lawyer, or whichever you want to indicate, I am really interested in whether you have any thoughts on that.

Professor Fraser Sampson: I am content and comfortable in both the official hats. There are two things at play here: people's fears about this and the technological reality. People's fears are quite often, in my experience, the bit that is getting ignored. The answer seems to be felt to be found within the technology, which it is not, because some of it is an emotional response. You can argue with someone as to why they should feel something, but they are unlikely to be convinced just by pointing to an algorithm and its functioning.

It is right that, as the technology improves, some of the areas that have gone wrong or have not been as accurate in the past will be getting better and cured. But anyone who engages with any form of electronic device, whether it is surveilling or measuring something, or a communication device, will know that we are a very long way off form it being infallible.

In fact, one area that I spent quite a while dealing with, back in 2021, was in a news report on the BBC on 18 October, whereby a woman's jumper was picked up by a traffic enforcement camera in Bristol. She had knitted it herself and it had the word "knitter" across the front. The camera issued a fixed penalty notice to a motorist in Surrey called Mr Knight, who had a cherished number on his vehicle, because the camera decided that that must be his vehicle, even though he was nowhere near Bristol. There are some really basic errors that we still see in this area.

Where you have people in the loop, they can generally be approximately right, but where some of these technologies are involved they can occasionally be precisely wrong in a way that no human would. Looking at that traffic lane in Bristol, for example, no one would have ever thought that was a car from Surrey being driven by poor Mr Knight, who was quite shocked to receive a fixed penalty notice.

Q3 **Chair:** That is very interesting. Looking particularly at biometrics and human rights—that aspect of your role—what powers do you have to oversee and challenge the use and retention of biometric data, such as fingerprints and DNA samples, and are the powers that you have sufficiently robust?

Professor Fraser Sampson: My answer is very short, because I have very few powers. The only real statutory power I have is in relation to national security determinations, which is where, under various statutes, the biometrics of individuals have been taken, usually on entering or leaving the UK. Even though they have no criminal convictions, there is an intelligence picture that suggests that retention is necessary—it is a very high test—in the interests of national security. All of those have to come to me. In the event that I do not believe they meet the statutory criteria, I quite literally have a red button that says, "Delete the biometrics". Beyond that power, I just have my voice and a keen urge to find an attentive audience.

Chair: What about your powers to oversee and challenge the way the police are retaining biometric data?

Professor Fraser Sampson: I have a responsibility to inspect. We do force visits where we look at how they are retaining samples and the processes in place for retaining biometrics taken in the course of ordinary policing operations. The powers are generally confined to an annual or periodic report to Parliament and what might, in some other setting, be called soft powers. I do not have statutory powers in that respect.

Chair: Do you think your powers are sufficiently robust? Remember, we are looking at this very much from a human rights angle.

Professor Fraser Sampson: I have not, so far, found the absence of them to be a problem, but then I have not yet come up against a hard stop where I am getting nowhere at all. I would probably need to be around a little longer than I have been. There certainly has not been an issue with getting the attention of the police and getting information back

in relation to biometrics. On surveillance cameras, I would say that is a different situation.

Chair: So you have a particular role in relation to national security. As I understand it, that is why your role on biometrics extends into Scotland, but the standard police use of biometrics in Scotland is covered by a different commissioner. Is that right?

Professor Fraser Sampson: That is right, yes.

Chair: Scotland has its own legislation covering that.

Professor Fraser Sampson: Yes.

Chair: Are there powers that you would like to have that might improve your ability to monitor human rights aspects of the retention of biometric data, such as fingerprints and DNA samples?

Professor Fraser Sampson: It might be more practically effective if those I am asking for information and explanation knew that there was an "or else". At the moment, they know there is not.

Chair: There is no threat.

Professor Fraser Sampson: No.

Chair: If you felt, in the course of your duties to monitor what the police are doing, that a police force was guilty of significant human rights breaches, would you report that to somebody?

Professor Fraser Sampson: Yes, I would raise that with the chief constable and the police and crime commissioner or deputy mayor for that force. I would report that to the Home Office. I have an ability, rather than a power—it is a statutory route—to make a report about any matters to the Home Secretary that affect my statutory functions. I have done that only once, and that was last November. That was not a human rights-related issue.

Chair: Would a report like that be made public?

Professor Fraser Sampson: That is probably a bad example, because it cannot be as it is a national security issue. Otherwise, yes, I would make it public inasmuch as I have a policy, which has not gone down particularly well with some camera manufacturers, to publish correspondence as soon as I send it somewhere.

Q4 **Baroness Kennedy of The Shaws:** It is nice to see that you are being reappointed to your role.

There are clear rules set out in legislation concerning how long DNA samples and fingerprints, for example, can be maintained and so on. That is about retention by the police. I wondered whether, in your experience, there is a culture of compliance with those restrictions or whether there is a default whereby they end up being kept when they should not be.

Professor Fraser Sampson: Yes, it is the second. It is really clear and it has occurred on every visit we make to every police force. There is almost a culture of having three categories: deleted, retained, and not deleted. Some of my input is to go, "If it isn't deleted, you've retained it, and if you retain it, you need to be able to point to an express power that allows you to and a lawful purpose for doing it", and around we go. I completely agree that there is a non-deletion culture.

Baroness Kennedy of The Shaws: There is a non-deletion culture. That has been my experience. Which ones end up being deleted? Which are the ones that the police merrily delete? The concern many have is that this culture of retention is, by creep, creating a national database. My DNA is shared by my three sisters. If you are keeping the DNA of somebody who has convictions or has done something that causes suspicion, in many ways you are keeping the DNA of the whole family.

Professor Fraser Sampson: Yes.

Baroness Kennedy of The Shaws: Some people might say, "All to the good. That's how we solve crime". But we want to know whether we are creating a national database by creep.

Professor Fraser Sampson: There are a number of policing databases, particularly for photographs, where that has happened. They are inadvertent databases. They have happened simply because you did not delete and you have more than one that is capable of being compared against things in the future. Essentially, you have created a database. From the police perspective, there is a great and probably growing anxiety that something in there may be critical to a future case about which the public will say, "Well, of course you should have kept it". It is not quite saying, "We'll hang on to everything just in case it comes in handy", but there is a quite proper focus on that. Look at some of the things that have hit public confidence in policing; if we had not retained certain things 20 or 30 years ago, we would be explaining something else.

Some of it is about balancing, but the principal difficulty is that they are operating where we are not talking about fingerprints or DNA; they are operating in a completely uncircumscribed world where we will not know until someone says they got it wrong.

Baroness Kennedy of The Shaws: The difficulty is that, on the one hand, the general public might be very cavalier about saying, "I don't mind people keeping it". On the other hand, if people are acquitted or investigated and there is no suspicion attaching to them, it should be deleted but it is not because it is retained.

One of the public's fears is that a database is being created which at some point in time might be used—with a malign purpose or even with a purpose that we have not been told about—to see who has signifiers for certain kinds of mental illness, such as schizophrenia or whatever. I chaired the Human Genetics Commission, so I know that there are not

many absolute signifiers of things, but there might be just a suggestion even that somebody is carrying a gene for something that causes alarm and despondency. This is where there should be a proper public debate about retention.

Professor Fraser Sampson: Yes, I completely agree. Even if we go back to the Strasbourg jurisprudence about record keeping by the police, which is pretty basic, the principles are the same, but the information—what you could know and record about that person—has magnified exponentially.

Q5 **Lord Dholakia:** May I follow up the question from Baroness Kennedy? Digital facial images are being collected by the police when a person is in custody. What is your view of the retention of records of this nature? Are there any regulations that allow you to say, "This is no longer necessary?" For how long can the police keep records of this nature?

Professor Fraser Sampson: This is a very topical area, and it is something that I look at whenever I visit any police forces. If you are arrested and passed through custody, your photograph and your fingerprints are taken. In the event that you continue through the system and you are then prosecuted and perhaps convicted, that is one journey. The problematic one is where there is no further action and you never come to notice again. That could be for any number of reasons, but the police still have your custody image.

That was challenged in the RMC case back in 2012 against the police rules for retention. The trial judge said, "You need to get rid of these. You can't retain them for people who have done nothing wrong or who are of no further interest". Your timeline for deletion should be months rather than years. I am here today saying that there are probably several million of those records still.

The response to that from policing and the Home Office is to say, "But they're retained on a database that doesn't have a bulk deletion capability". I am not sure that works for public trust and confidence, but even if it did it does not work for the Strasbourg jurisprudence in Catt that says you cannot rely on a flaw in a database that you have built for unlawfully retaining stuff about me.

It is not just a problem because of the images and the individuals on a database who might find themselves, for example, being used on video identity parades that they did not know about because there would be no way of letting them know. All these routes come back to public trust and confidence where they say, "Okay, if this is what has happened for the last 10 years and here is what public challenges in the courts have said, and it still isn't right, how are we going to have trust and confidence in what you're proposing with new technology that will tell you far more about us?" That is one of the questions that I put.

I understand that it is a technical problem, but it is of the country's and the police's making, rather than the people whose images you have kept.

Lord Dholakia: There has been a lot of controversy about methods such as stop and search. I am not saying that images are taken at that particular stage, but that sort of controversy where a person found out that his images are kept would discredit the police in the way they are behaving on this particular matter. When you bear in mind that people's facial expressions change over time, do you think there must be a stage beyond which such images no longer ought to be kept?

Professor Fraser Sampson: It is certainly a valid challenge. There are people who would say, "Our algorithm is capable of ageing you automatically. We can see what you'd look like in 10 years' time and what you looked like previously". Again, that needs proper discussion and understanding, and the public's acceptance of that as a proposition.

In terms of public space surveillance, we are now moving from a world where the police relied on images of the citizen when they passed through custody in very controlled settings to one where they are increasingly relying on images from the citizen, sent in from dashcams and GoPros. That is often one of the first requests to come from a police force following an important incident: "Would you please send in anything you have?" The material that is then available to them to sort and assess against the standards, and then to decide whether to retain, is increasing significantly without any real rules or legislation beyond the internal guidelines for the retention of data generally, which I am not sure goes far enough to assuage the concerns that you have just outlined.

Lord Dholakia: A person in police custody is not necessarily a guilty person. The process has to be gone through. Is the person told that his images are being retained by the police, or how does he find out that there is something more than being discharged from the courts?

Professor Fraser Sampson: That is one of the points that we make on our visits to forces. More starkly, under our constitution, unless they have been convicted, they are presumed innocent. Therefore, on what basis would you retain their photograph if there is no prosecutorial process that will follow on from it?

Some police forces have started issuing discharge information packs to people released from custody. They do this in Yorkshire and the Humber, where they say, "We took your photograph while you were in custody. In the event that we don't proceed with you, you can ask for that to be deleted". But the onus is still on you, and whenever you are in custody, whether you are coming in or going out, you are probably focusing on a lot of other things as well. Most forces we visited just say, "Look on our website. If you want your photograph deleted, you can apply". That goes back to the culture of non-deletion rather than "delete unless".

Lord Dholakia: Are there any good international practices in this particular matter?

Professor Fraser Sampson: I am not sure about international ones, but I know that the PSNI does not have this problem, probably because of

the IT arrangements. Northern Ireland has a much clearer link between the prosecution and investigative process and outcomes, and people being able to delete their own photographs. But they work in a single force area rather than across England and Wales. They do not have this problem.

Chair: You mentioned that sometimes people who have been through custody processing and who have not been convicted have their images kept and used for video identity parades. Unless we have a rule saying they should not, there is perhaps an incentive for the police to hang on to these images, because they can use them for video identity parades.

Professor Fraser Sampson: Yes, I can see that there would be an incentive. If you couple that with the question, "Where is the requirement for me to do so?", you are erring on the side of not getting into trouble because that was the one photograph from 3 million that turns out to be the one you should have kept. The numbers are so large now. Again, this is all about public trust and confidence. The more we are able to do with surveillance technology in the future, the more important it will be to say to the citizen what we are not doing with it and for the citizen to be able to rely on that assurance. We are a long way from that.

Baroness Kennedy of The Shaws: The system is set up in a way that basically puts the burden on the member of the public to be wise enough, or to have a good enough memory of what happened at the police station, to remember what was in that thing that they signed at some point and that they have the right afterwards to apply to have the thing deleted. If no application is made because people are just saying, "Oh, thank goodness that's over", the thing remains on the computer and there is non-deletion. There must be a concern here about where that is preferred. I mentioned the business of how the information of a whole family, if it is DNA that is being retained, is basically on the database. Have we ever analysed this to see whether a black guy is more likely to have his sample kept, because they will think, "That means we have the whole family on the database"? Does that happen? Is there a risk of that?

Professor Fraser Sampson: I do not know that that evidence is available, but another really important factor is that, as well as having the wherewithal, the capability and the understanding to make the application, you need to have confidence that it will make any difference and that it will be done. We are back to people thinking, "Is it worth it? Why would we bother?", unless they have some confidence that making that application is worth the candle. Some groups may have less confidence than others in it making any difference and being heeded.

Q6 **Dr Caroline Johnson:** You talked about the non-deletion culture and people's worry that, if that particular record was deleted, it could be the record that solved or prevented a crime or caught some particularly egregious criminal. Is there any evidence of that happening? Is there any research into how often data that was not deleted when it perhaps ought to have been has been key to resolving or preventing some sort of crime?

Professor Fraser Sampson: Not that I am aware of. That is the approach that you might expect, for them to see whether that reinforces at least the basic premise that one day it might be worth doing. The closest we have come to it with my powers is under Section 63G of PACE, where you can apply very specifically to retain the biometrics—fingerprints and a DNA profile—of an individual who has been arrested for a certain qualifying offence but where there has been no further action. Those are usually cases of domestic violence where there has been a reparation in the relationship, so the complainant withdraws their statement, or of gang-related violence where there is some form of intimidation, so the person, if they want to carry on living in that area, retracts their statement. In those cases, if you are the chief officer you can make an application to me to retain it for three years. We still have very little information about whether those retentions helped to prevent or investigate crimes that were subsequently committed.

Dr Caroline Johnson: There has not really been research in that area.

Professor Fraser Sampson: No.

Q7 **Dr Caroline Johnson:** I also want to ask you about your national security determinations, where you are able to retain data lawfully for five years on a rolling review basis. How often does that happen? What is the volume of people?

Professor Fraser Sampson: When I first came into the role, there was, perhaps understandably, a significant backlog from the Covid-19 pandemic, because everything had shut down almost completely, so I needed to get through that backlog. We are probably back to a normal rhythm now and I see about 50 or 60 a month.

Dr Caroline Johnson: What proportion of those retain the data?

Professor Fraser Sampson: Almost all of them do. My part in the process is to challenge. I have an ability and an agreement that I will challenge them and say, "The chief officer's comments here don't address necessity or proportionality of the determination being made or the period over which it is to remain in force". If I challenge those, the chief officer who has made the determination will then come back and say, "On reflection, three years seems proportionate", or sometimes, "We don't believe we've met the necessity criteria and therefore we don't need it". That happens very rarely. As often as not, they say, "Thank you very much for your observations. We're keeping it".

This information is classified as secret, so the individuals will not know that they are subject to a national security determination. Their ability to challenge it even in the courts will be very limited, because they probably will not be able to get to the information. The office and I are the only ones standing between that individual and the machine that is deciding to keep their biometrics and probably share them elsewhere.

I am quite keen on pushing back in these areas where, if the person had been able to make representations, they might argue it. There are some

really obvious ones to me, such as references to people's faith, religion and belief. As a freestanding point, that is a human right. That is not a reason for retaining.

Dr Caroline Johnson: Which particular human rights challenges are posed by the retention of this data?

Professor Fraser Sampson: Principally, the most practical one is movement, because some of them are for people who are not in the UK, and, were they to return to the UK, there would be a significant national security risk. There are freedom of movement considerations there. If you are already in the UK, the principal issues will be privacy and right to family and home life, as well as Article 14, if the system is biased or discriminating against you in any particular way, possibly in the way they have been arrived at. I go back to the one in the last 12 months where the chief officer's reasoning included, "Given this person's clear and strong faith", and I sent it back saying, "This person is entitled to a clear and strong faith as a matter of settled law. How is that a basis for seeing them as a threat? If that's not what you meant, don't put it".

Beyond that, if the explanation is written in the right way by the chief officer and I simply have the intelligence picture to go on, I do not really have anywhere to go. The challenge is binary: it is either delete or approve.

Q8 **Lord Alton of Liverpool:** Professor Sampson, the last time we met, it was to discuss the proposal to abolish your office. It would be interesting for the committee, at least in parentheses, to know why they thought it was a credible proposition to abolish the office and how you convinced them to retain it.

I want to ask you a very specific question. You referred earlier to Article 8 of the European Convention on Human Rights, specifically the safeguarding of information that might affect an individual's or a family's right to privacy. Back in 2022, your role as Surveillance Camera Commissioner was merged with the role of Biometrics Commissioner. How effective is the surveillance camera code in protecting those rights, and are the penalties sufficient when those rights are not observed?

Professor Fraser Sampson: The first one is very straightforward. I have not managed to persuade the Home Office of this or much else. I certainly have not managed to persuade it to abandon scrapping the code, which then means that you do not need a Surveillance Camera Commissioner. It is simply that the legislative process is taking rather longer perhaps than had been planned, and certainly longer than my appointment. The plan in the Data Protection and Digital Information Bill is to delete the requirement for the Government to publish a surveillance camera code, so you do not need half of me. That still obtains; that is on its way through Parliament. I agreed to be reappointed while that carries on on its legislative journey, but the policy intent remains fixed.

In terms of the policy intent itself, policy is a matter for others. My job is to oversee compliance with the code and to advise on it, which I do. The code, as you will know better than I, was required by Parliament in 2012 as an additional layer to general information and data protection controls, given that the people using it were the police and local authorities with investigative functions. It was seen as an additional layer that was needed, given the consequences.

At the time the code was introduced, Edward Snowden was still a trusted contractor for the NSA. I have yet to see anything that has happened over the subsequent 10 years to indicate that we need less regulation on state surveillance in public spaces or anywhere else. We probably need better regulation. Scrapping the code will mean that the single instrument that directly regulates the police and local authority use of public space surveillance will go.

In terms of the effectiveness of the code, it is a very good instrument, although it is incomplete. I tried to get a small sentence inserted last year that said, "By the way, do it ethically". That was not to be done. It regulates, in some great detail, how surveillance operators should use their systems responsibly, in a way that the public would rightly expect and that retains their trust and confidence. I know that, because that was a paragraph that I did manage to get in. Applying it only to police and local authorities does not make a lot of sense to me. There is a clear alternative—I put this in my public response to the consultation—for the Government to adopt that code themselves across the government estate, for example, which has caused some concern in the past.

Retailers increasingly ask me whether they can adopt it and for advice on how they would do so, because it makes a great deal of business sense for them to do so. It goes through everything from training and standards of the equipment to who you can share it with and the minimum levels of intrusion. It reinforces the relevant articles from the convention and underpins the general data protection principles. It is an instrument that works. It has not been challenged successfully, or at all, in the courts. It is a government instrument and people have got used to it. There are no penalties for failing to follow it, but it can be and will be taken into account by a court in the event that it is relevant in proceedings, as it was in Bridges.

On Article 8, it covers off some of what we might loosely call privacy considerations, but it would need to go further if it was to stay around. Part of the difficulty I now have is knowing that the code is on death row. It is simply waiting, subject to the will of Parliament that it will be gone and we will not have one. I cannot put a great deal more effort in through the team to say how we might adjust it or tweak it.

Lord Alton of Liverpool: The Information Commissioner, John Edwards, this week spoke out about the tragic case of Nicola Bulley in Lancashire and said, "Data protection law exists to ensure people's personal information is used properly and fairly". He has said that he had now asked Lancashire police to review its decision about some of the

information that has been disclosed and that has caused such distress to Nicola's family. Do you link with other commissioners like him in making sure that we have effective responses in cases like that?

Professor Fraser Sampson: We work with the Information Commissioner's Office. We have regular update meetings. At the moment, the ICO's position has been that we have this covered in terms of surveillance cameras for public spaces, so any guidance it produces does not duplicate anything that we might do.

There are matters arising from surveillance practices that are not covered by the general data protection regulation. A clear example would be the offending of double murderer David Fuller, who, as well as committing two murders, sexually abused, they estimate, over 100 corpses in mortuaries, filmed himself doing so and retained the footage. Had he conducted a data protection impact assessment before making those hideous films, data protection would not have been engaged, because it only protects the rights of the living irrespective of the distress that it might cause to relatives. The same will be true of the police officers who were properly sacked for taking pictures of murder victims and sharing them. In terms of data protection, again, you are back to an identified living person. What that means for the future and our increasing capability for surveillance I do not know. Again, policy is for others, but it is not all covered by data protection.

Q9 **Baroness Kennedy of The Shaws:** I know it is very difficult. You do not want to step outside your position and make statements about policy, but it seems that there is a sort of fetish about deregulating that stretches even into your arena. Is that your sense?

Professor Fraser Sampson: Yes.

Baroness Kennedy of The Shaws: That is why this legislation is on the table, because we are getting rid of regulations, yet here is an area where, quite clearly, regulation is vital. The code might also be vital in areas beyond that which we are looking at here to do with policing, security services and so forth. It might be about banking or all manner of areas where these things are going on, for which codes can remind people of the ethics and the responsibilities to protect and so forth. We really are playing catch-up with so much to do with technology, and law and regulation are often behind it. Are you in a position where you can say to government, "I really think you are making a terrible mistake in going down this road"?

Professor Fraser Sampson: In my public response to the consultation, I have proposed some alternatives. The original consultation was on whether everything, including the biometrics functions, should be "absorbed"—that was the language—into the Information Commissioner's Office. I and others said that to ask that question reveals a misunderstanding of the role. My role as biometrics commissioner is quasi-judicial. If it needs to go anywhere, and I do not believe it necessarily does, it should go to the Investigatory Powers Commissioner,

rather than a data regulator. That is now in the Bill, but there is no absorption or transfer of the residual part for surveillance cameras and surveillance functions in public space by policing and local authority. It simply comes to a dead halt on Royal Assent and the Bill coming into force.

Baroness Kennedy of The Shaws: It is very clear that you have acquired a real area of expertise in your particular area. To imagine that it can be easily absorbed by somebody who deals with other forms of data, it seems to me, is a total misconception of what you are actually doing.

Professor Fraser Sampson: I think so. One thing I have said a number of times in a number of forums is that, yes, biometric surveillance involves the processing of data, but so does almost every other meaningful activity in life, in the way that, if it involved electricity, we would give it all to Ofgem. There are consequences here about who is doing the processing. If it is someone or a body with a law enforcement or investigative function, that is very different from a lot of other areas of data protection. In my view, live facial recognition, for example, is no more just data protection than DNA profiling is just chemistry.

Q10 **Bell Ribeiro-Addy:** We have been talking about what the impact might be. What impact do you think the abolition of the role will have on safeguarding of individuals' human rights?

Professor Fraser Sampson: By removing not just one layer of regulation and standards but the only bespoke layer—it is the only direct instrument for this—it is reasonable to assume that it will dilute some of the specificity around the concerns that we have been talking about. Perhaps more subtly, it will indicate the direction of travel towards a culture where, if nothing says that we cannot and no body asks, "Why are you doing it?", we will head more in that direction.

A feature that I am starting to see increasingly in my role is that when people are asked, for example, "What is your view on live facial recognition for school lunches?"—to take a topical example that is not mine—people generally approach it the wrong way round. They say, "I don't really see anything wrong with it, but should I?" As the technology becomes more sophisticated and increasingly difficult, and some of the legal issues become embroiled in that, you need regulators that can help you to form self-challenge questions. At the end of those, you might still be satisfied and say, "Actually, I'm all right with it", but at least you got there by a rational, evidence-led, risk-based conversation, rather than thinking, "It feels okay. What are the things we should worry about?"

When you start to produce a list of things that you should check off—for example, some of the questions we have had here—people then say, "Actually, I'm not sure now that I was comfortable with that at all". There is probably a role in the future, as technology increases and becomes more fiendishly clever, for all regulators to say, "Here are the ways of kicking the tyres for yourself before you form a view", rather than you

intuitively saying, "I can't see what is wrong with it. Can you tell me?", if that makes sense. That would be lost as well.

Q11 **Bell Ribeiro-Addy:** With the Bill stalled at the moment—as you know, it is waiting for its Second Reading—how difficult is this making it for your work and ability to prepare for the future?

Professor Fraser Sampson: It is certainly challenging. When I agreed to reappointment, it was, and remains, directly tied to the fortunes of the Bill, so my reappointment is up to Royal Assent plus three months, or 15 months. When we had that conversation, Royal Assent was planned for this May. Since agreeing to reappointment on that basis, I have learned from the Bill team that Royal Assent may well be next May, which prolongs the period. The way I saw it—and I have some of the team here with me—was to say, "I know it's kind of difficult motivating you to come back after Christmas and take down the decorations". The longer that takes, the harder it will be, but we will keep doing this full on until Parliament says otherwise.

Bell Ribeiro-Addy: It has not had a significant impact on what you are carrying out, in that in some ways it seems like you are almost waiting for responsibilities to be removed while trying to carry on doing the job.

Professor Fraser Sampson: No. Really interestingly, most people I engage with in policing and local authorities do not even know that it is on its way through the House. It is news to them, so it has certainly not been problematic—in other words, by people saying, "You won't be here for much longer, so why are you coming?"—because they do not know that it is going through the House.

Bell Ribeiro-Addy: If the Bill goes ahead eventually, what specific recommendations, if any, would you have for the new Investigatory Powers Commissioner? How do you think that role should operate?

Professor Fraser Sampson: We are already talking to the office, and I have spoken to Sir Brian Leveson a couple of times to say, "It makes sense for us to start looking at the practicalities of this". There are some really straightforward ones; for example, is it even ready to be handed over, in terms of the software? I have put in my annual report that the software for running national security determinations is lamentable, really. Even the records I endorse are wrong on the face of it, because the capability to amend does not exist.

We are back to the custody photos a bit here. You have built a system that it is run on, and if the original decision was that it would be for five years and then we agree with the chief officer that it is better for it to be two years, the formal record still says five years because it cannot be amended. The field that says which piece of legislation you are using will not cater for recent law from Parliament. It says that it will be a Schedule 7 on the capture of biometrics when in fact it is a Schedule 3 on hostile state acts.

This is really important activity. I am not here to speak for Sir Brian Leveson—heaven forfend—but I am trying to indicate to policing and the Government that it would be a very interesting judge who would just say, "I'll sign this", knowing that it is utterly wrong on the face of the instrument that they are signing. So far, they have been quite lucky that I am prepared at least to go along with it because I understand the flaws.

That would deal with the biometrics, because that has a destination for the Investigatory Powers Commissioner. The surveillance camera code has absolutely no further information around it, not just in the Bill but in my office. We have no idea where any of these responsibilities might go.

Bell Ribeiro-Addy: We are completely unprepared at the moment, should this Bill go forward.

Professor Fraser Sampson: That is a fair assessment for the surveillance camera part, yes.

Q12 **Baroness Lawrence of Clarendon:** Good afternoon, and thank you for coming. As Lord Alton was asking his question and you replied, I was wondering who regulates the regulator.

Professor Fraser Sampson: There is nobody, from what I can see. I am an independent public appointee. I am appointed by the Home Office but once I am here I am here. I am subject to the same public law challenges and jurisdiction that any other public body would be, but it is just me.

Baroness Lawrence of Clarendon: That is like a judge. My question is about human rights organisations, such as Article18 and Liberty, which have highlighted that there is mass surveillance, which has a chilling effect on freedom of expression. Do you think that the UK's current use of surveillance strikes the right balance for the purposes of Articles 10 and 11 of the European Convention on Human Rights, which protect the freedom of expression and the freedom of association?

Professor Fraser Sampson: I am not sure we can demonstrate that it does. There are activities that are regulated, for which I have some oversight functions, although they are very low and limited. If you take the overall public space surveillance activity and the aggregated surveillance capability that is relied on let us say for policing, I am not sure there would be the evidence there to say that that meets all those requirements.

One thing that I believe the state, and in particular the police, ought to be able to do is to answer that question and back it up. If you were to say, "The capability currently exists for extraordinary amounts of vehicle data to be collected through the automated numberplate reader system", layered on top of that there may be a capability for identifying individual device information from phones in a vehicle. Layered on top of that there may be other intelligence patterns that say, "The person who was seen at protest X was also seen at protest Y".

Taking those things together, to what extent would people rightly worry that if there was to be a further protest in the future, there would be some form of tracking to see whether they were going to attend, such that they would not go if they were to find out? Even if they could not get an answer to that, would they decide not to go or not to use public transport? Our capability to intrude on people's lives is so great now that we need to do a lot more and expect an evidence base to answer that question. Without it, we are guessing, and my guess is "probably not".

That is when we are dealing with temporal issues. We then start talking about predictive policing, pre-criminal activity and tracing potential witnesses, which the College of Policing spoke of. I do not know what a potential witness is. I think it is a member of the public. Once you layer all those together and people do not get a satisfactory answer—you might not being getting one from me now, because I do not have the information—they may lose faith in that system. That is what it takes.

Baroness Lawrence of Clarendon: Looking at mass surveillance, back in 1999, when a lot of stabbings and things were happening, one point from me to the police was about how, by having CCTV and surveillance around areas, identifying the perpetrators would be quite easy for them. That never seems to have happened, so there are a lot of victims where crime has happened. When you think about mass surveillance, to me, that is part of what I had expected to happen: if police are looking at surveillance, they will be able to see all that. For me, it seems as if they choose what they want to see and go after whoever they think they should at that time. When the police are looking at surveillance, how often do they use the camera in the way they should—in order to catch the perpetrators who are committing the crime?

Professor Fraser Sampson: Some of the very real and practical benefits to policing of the technological developments here come from AI-driven video analytics, which can cover vast amounts of images and CCTV footages retrospectively. The event has happened and been recorded, both as a crime and, technologically, as images. The scale of the capability to point an algorithm at that and say, "Try to check these faces against known criminals who are involved in that area or that crime type" is—I do not like the expression particularly—a game changer for policing.

Policing is just starting to use it. I think that it will, and should, use it much more for looking backwards at things we already know were committed. They are plainly crimes. They had victims. All that is preventing us from being able to identify the people who were caught on CCTV, when that is the principal purpose of putting a camera or cameras there in the first place. Until now, it has been very difficult to knit together images from different systems all at different times in the way that is perhaps portrayed in fiction. Now we are getting very close to that, and in some circumstances you can run that through very reliable comparisons in quick time, so you do not have to sit and go through it.

One by-product of that, which we need to look at because it is still too early to know how that will impact it, is that unless the rest of the investigative system moves at that same new speed, you will simply create a bottleneck of things where you have identified a lot of people historically with some new AI but you need some investigators to follow it up. If you have the same number who were dealing with manually spliced video tapes, it will not have contributed much to the overall investigative capability.

Q13 **Lord Alton of Liverpool:** One of the responsibilities you have concerns national security. You will know that the Procurement Bill is going through Parliament at the moment; it has completed its stages in the Lords and is currently in the Commons. For the sake of transparency, when it was in the Lords I moved the all-party amendment—I think you are aware of this—specifically on surveillance cameras being manufactured by companies, such as Hikvision and Dahua, with direct links with Xinjiang and the persecution of Uighur Muslims, 1 million of whom are thought to be held in the camps there.

As you know, the amendment obliges the Secretary of State to publish a timeline for the removal of physical technology or surveillance equipment from the Government's procurement supply chain where there is evidence that a supplier has been involved in modern-day slavery, genocide or crimes against humanity. In your view, does the use of equipment supplied by states or companies involved in human rights abuses, or that clearly have credible links with such abuses, have any implications for the UK's compliance with our own human rights obligations?

Professor Fraser Sampson: Yes, in a number of ways. In terms of the nexus between the development and the deployment of the surveillance capability itself, this is not about the statutory and standard response from some providers that, "We sell cameras". If that company has been involved in the design, building and operation of those camps, to say, "We simply sell cameras and can't be held responsible for what they are used for" has profound implications for our buying it at all and probably still more for our buying it for our police to use.

When it is used by that state, through the police, to identify individuals, using algorithms that purport to be able to guess their ethnicity and racial or cultural heritage, intern them in those camps, torture and interview them while they are filmed with those same devices, and then subject them to all the other appalling treatment that the Foreign Affairs Committee set out very clearly in 2021, I cannot think what business we have even contemplating handing them public money. If we are going to, as a starting point we should probably have a public debate with the people whose money we are using and ask them to what extent they are okay with that.

We fall a long way short of our being able to demonstrate as a state that we have complied with the UN principles on fundamental, universal rights. Pointing to an absence of any clause in a procurement process in

local policing that says, "There's nothing here that says we can't", is completely ducking what I accept is a very difficult issue. Again, I come back to the point of public trust and confidence. If we as a nation expect our citizens to put trust and confidence in the way our police use increasingly intrusive technology, we need to recognise that if there is nothing in the procurement arrangements that we follow before buying that stuff and giving it to our police officers, maybe our procurement rules are wrong, rather than the principle being okay.

It is kind of surprising, as well as a little saddening, that backstage I have yet to meet local authority representatives, chief police officers and others who disagree with me. As soon as the curtain goes up, I am on my own in the spotlight and the police give out prepared statements saying that there is no procurement breach. We cannot maintain that position for long if we are going to say to the public, "You have to trust us in the way in which we use this equipment".

On the link between the companies mentioned in the Foreign Affairs Committee report and the state, I have asked those companies these questions and they have not answered them. I have asked, "Do you accept that these things are taking place in this part of China, and would you explain the extent of your involvement in them?" That tells me that this is the state operating behind the veil of incorporation. This is not even dealing with a straightforward global provider of surveillance technology; this is dealing with a company that is not allowed to answer my questions.

I am guessing that, had I asked these questions of probably any other global surveillance provider, you would not have been able to stop them coming forward and disavowing those things, or presenting the evidence to show, "We are in no way whatever connected with those events". Given that they have not answered my question "Do you accept this, and to what extent are you involved?" for two years, it is reasonable to conclude that they are a state-controlled provider.

Lord Alton of Liverpool: Are you able to share that correspondence with the committee, because it would be very helpful for our report, if it is in the public domain?

Professor Fraser Sampson: To the remarks I made at the beginning, that is what I do. In order to remove any suggestion that anyone could have sought to influence the content of it, I publish my correspondence as soon as it goes out. There is my letter that says, "Dear Hikvision", and its complaint, which says, "Would you give us time to think about this before putting it on your website?" No, I will not, actually. Room for manoeuvre here is fine. The need for trust for me is really clear, and it says, "There can be no opportunity for you to do this".

Again, on freedom of information and freedom of expression, last year I was asked by a security journal in the UK to write an article on biometric surveillance of my choosing. I chose to write about the use case that I thought was there for live facial recognition in policing. I presented it for

publication to *Security Journal UK*. When I got it back for proofreading, one paragraph had been excised. I asked, "Have I breached some word limit that I was unaware of?" They said, "No, we've taken out the bit about Hikvision". I asked, "On what basis?" They said, "They are our principal advertiser". I said, "Send me my article back".

If you are allowing classifieds to affect content, first, that is not journalism, but, secondly, you are not having anything I have written. I published it in *Tech Monitor*. I present that as evidence, because if that is the level of control you have over our publication in the sector in the UK, I am going to be a lone voice for quite a long time.

Lord Alton of Liverpool: That is deeply disturbing. The surveillance state in Xinjiang is something that we should all be deeply apprehensive about. This committee obviously is mostly concerned with the implications for our upholding of human rights in the United Kingdom. We are signatories to the 1948 Convention on the Prevention and Punishment of the Crime of Genocide, with its duties to prevent, protect and punish. Are you saying that you think we would be in potential breach of those obligations and our obligations as a signatory to the Universal Declaration of Human Rights? Are we in breach if we do not put in place the kinds of procurement policies that you say we should?

Professor Fraser Sampson: There is a very real risk that we are. I do not separate this, as others have, into security of data, where it is going and who it is being shared with, and the ethical and human rights issues, because they are of a piece. If you have any reason to believe that data about anything from those systems is being shared improperly—or at all, because you have not agreed it—with a state that does not necessarily wish us well, there is no room for further discussion.

The Government accepted that these systems had to come off very sensitive sites. Of course, that does not answer the question about how on earth it got on to those sites to start with, if they are our most sensitive systems. Given that admission now and the fact that those systems have been taken off, that tells me that we as a Government accept that some of that data and those images cannot be controlled in a way that we would like. Therefore, we move closer to that risk materialising that you have identified. Simply focusing on saying, "It isn't plugged into the internet", or whatever else people are saying, does not deal with it for me. Then we come back to the question: if you are not in control of that, why is it in our high streets? Why is it in our schools? Why is it in swimming pools, libraries, supermarkets and anywhere else?

Chair: This is a very interesting issue: the degree to which the United Kingdom is complying with international treaties in what is happening in the United Kingdom, which is what this committee focuses on.

Baroness Kennedy of The Shaws: It is very much United Kingdom-based.

Chair: We do not look at international human rights. People often want

us to look at international human rights issues, but that is not within our remit. Clearly Lord Alton's questions are within our remit, because they go to the extent to which the use of this equipment in the United Kingdom is compliant with our human rights obligations.

I am interested in your mention of the United Nations. Later this year, this committee will scrutinise the Government's response to the universal periodic review. These issues about how our trade and business relationships with other countries impact on human rights, both abroad and in this country, will be part of that. It is something that we will really have to follow up on and get our teeth into.

I am conscious of the time, and we have a little more ground to cover. Lord Alton, did you want to add anything to that?

Lord Alton of Liverpool: No, I am very grateful for what Professor Sampson has said. If the correspondence can be made available as well, we can include that.

Chair: You have raised some very important issues there, Professor, and we are very grateful to you.

Q14 **Baroness Meyer:** Thank you for being here. It is fascinating. I would like to move a bit towards regulation. From everything you have said, you probably do not believe that the current regime makes the UK compliant with our human rights obligations. As such, you probably believe that we need a regulator. What powers do you think the regulator should have? Have you been speaking to the Government about this? What are the hopes of this happening?

Professor Fraser Sampson: To take the last question first, yes, I have frequently spoken to the Government about it. As to whether anything is happening or what should be happening, we need regulation to reflect the reality of the area being regulated and for it to sit where people would intuitively expect it to be found. A lot of the regulatory activity that we do in the office is answering people's "What if" questions, or "How does this look?", rather than reporting and then intervening in some form or taking punitive action. It is more about answering questions about why this is happening and the things that we should be concerned about, whether they are allowed to do this, and where we go to get more information.

At the moment, people are generally quite clear that, if it is about public space surveillance systems, they come to our office. A lot of the time, we say, "Actually, it only has to be adhered to by local government and the police, but here are the principles in any event, because, if any other regulator were to produce this, the list would probably be very similar".

It is about where you intuitively look for it. Were the Home Office to be here, it would say, "Policy intent is to simplify, so make it more intuitive so that people understand where they go. Therefore, the fewer regulators and commissioners, the better. This is all about data, in which case you would go to the UK data regulator".

I understand that, in the Bill that is before Parliament, only the bit that appears right at the end before the printer's name is about us. All the rest of it is about reforming the Information Commissioner's Office and functions. I do not know how far, within those revisions, there would be an expectation for a newly constituted data regulator to pick up on this. As we know, we do not have a freestanding right to privacy here, and we do not really then have a privacy regulator. It is kind of an Article 8 expansion, and I query whether the capability for intrusiveness on an increasingly covert and very large scale means that somebody should think about that as well. The world is moving very quickly and we are still dealing with analogue rules.

Baroness Meyer: If we compare the extent of the regulations in the UK to other democracies, where do we stand?

Professor Fraser Sampson: That is interesting.

Baroness Meyer: I am not talking about China. I am talking about Europe.

Professor Fraser Sampson: Actually, China is one of the most heavily regulated surveillance users. Do not confuse regulation with ethics. Yes, there are countries that will have regulators that oversee their privacy rights. Where those are particularly or specifically enshrined, there are countries where it is a subset of a broader data regulator's role. There are those that have freestanding biometrics commissioners. Israel, I think, is an example. I have met with the Israeli counterpart.

I spent probably more time in 2021 and at the beginning of 2022 briefing Australians about our risks, principles and systems than I have at home. I can say with some confidence that the Australians are very interested in having biometrics—facial recognition, gait, voice and anything else all in the same thing—because they are all used by those same agencies for the same purpose, which is to identify people and look at what they are doing. They were really interested that we have a joint commissioner for now. I did not really have the heart to tell them that we will not have for very long.

Q15 **Chair:** The Metropolitan Police has started the operational use of live facial recognition technology. In your view, what implications does that have for human rights?

Professor Fraser Sampson: There are significant implications because of its potential for intrusion technologically and the perception of how it is being used societally. If we had looked down the road 20 years ago and asked, "Which of the following technologies is most likely to engage serious human rights concerns in policing—Taser or surveillance cameras?", I do not think most people would have got it the right way round. Yet we introduced the Taser into policing, which is the deliberate application of a high-voltage electrical current to a human body in order to gain compliance. There are some significant human rights issues engaged with that new technology, but actually, in the way in which it

was introduced and is now deployed, it is seen as very helpful. It is less than lethal, and there have been few, if any, challenges that I can think of relating to it being misused.

But just because it does not hurt does not mean it is not harmful. We need the same level of sensitivity in the introduction, monitoring, learning and abandoning—in the light of the raw input of reality, as people have called it—of surveillance. It is not just the Met; we are struggling against perceptions created by exuberant early adoption here and in other jurisdictions, such as the United States.

We are also struggling against the data that was produced in 2015 or 2014 from some very early trials. You will still be presented with that data if you are the Met Police Commissioner. In technological terms, it is the Pleistocene era; you are being shown a fossil. It is quite proper that you are shown it, but you need to be able to demonstrate how algorithms have got so much better and are so much more reliable.

There are use cases where it would be appropriate for policing to use live facial recognition. There are times when the public might expect it to be used. There is a very important distinction here between policing and law enforcement. The language across the Atlantic has conflated them. Law enforcement here is a function rather than a sector. Policing is much bigger than law enforcement in the UK. The use in policing for safeguarding or finding vulnerable missing people, which is very resource-intensive and could benefit from intrusive surveillance technology, will probably attract more public support than its use for catching people or enforcement. The law enforcement element is probably the area that is least likely to attract public support and most likely to cause public disquiet about intrusions into privacy, home and family life, discrimination and all the other rights that we have discussed.

Chair: I wonder if I should bring Bell in here, because there has been some alarming research into aspects of discrimination and bias under the use of live facial recognition technology. I do not want to anticipate what you are going to ask, Bell.

Bell Ribeiro-Addy: That is exactly what I was going to ask.

Chair: I thought you might want to ask about that.

Q16 **Bell Ribeiro-Addy:** We have discussed how it can be a very important tool, but a lot of evidence points towards the fact that this facial recognition cannot distinguish between black and Asian people. Sometimes it misrepresents their gender or just confuses them entirely. The technology is just not good enough for that. Something similar is to be said when it comes to the collection of DNA because of the well-known reporting of racism in policing. Black men in particular are more likely to have their DNA collected and so stored. I wonder how the challenges of this are being dealt with.

Professor Fraser Sampson: All that is essential upstream challenge for those who are even contemplating using new technology. As for the way

in which the technology itself works, I have had people say, "Our AI algorithm is so complicated in the black box that we can't explain it". If you are expecting public money, you need to be able to explain it. If you are going to deploy it in a way that meets the public sector equality duty, you had better be able to explain it. If you are to attract the trust and confidence of the community who bought it and are being subject to it, you need to explain it.

The technological challenges, including the complete—to a statistical level of importance—absence of bias or inappropriate technical functioning is on you to produce, publish and keep under review before you even think of using it. The way it is deployed then is a different issue. If it is another tactical option and operational tool, you should expect the same level of challenge on the way you deploy it, on which groups, to what effect, and with what reason, as you would have for anything else.

Those conversations need to have been had very early on in the discussion and certainly pre procurement. I cannot comment on the extent to which they are being had, because I am generally not invited to those discussions.

Bell Ribeiro-Addy: Would you have expected that it would be part of your function to be able to intervene in a matter such as this?

Professor Fraser Sampson: Yes. It would make sense to invite the office in. I have had very productive meetings, on a voluntary basis, with a Metropolitan Police commander, looking at road safety and how we might be able to assist, with our office advising and pointing out areas for consultation, challenge and red teaming well before there is any move towards deployment. He and I thought this might be a good proof of concept and a very sensible way of working, absent any statutory changes or powers, because it is the right thing to do if you are to get the results you want with community support.

Bell Ribeiro-Addy: My worry is that, despite the fact that we have all this evidence and a regulator, there seems to be no one who can prevent it being rolled out, even though we know that it is behaving in a manner that does not work for all of society.

Professor Fraser Sampson: Yes. From a purist point of view, revisiting some of the questions in the discussion we had earlier, if the Government are right that this is simply a matter of data protection, or an extension of data protection, we have a body already, our data regulator, which has some significant powers of intervention and punishment. I am unaware of any intervention that data regulators, not just in the UK but in any GDPR jurisdiction, have made in the police use of surveillance and the intrusive use of surveillance.

Bell Ribeiro-Addy: Do you think it would make more sense to sit with the regulator, given its role?

Professor Fraser Sampson: Yes.

Chair: Should it sit with you?

Professor Fraser Sampson: At the moment, yes. I go back to where intuitively you would look to it if you wanted to ask someone those questions.

Q17 **Chair:** I have a more general question to end with, Professor. What should the Government's priorities be in their forthcoming artificial intelligence White Paper on safeguarding human rights protections?

Professor Fraser Sampson: The priorities ought really to be to understand very clearly all the risks associated with that technology, not just now but the potential application of it, and to get some very sound technical advice on what can be done with that. If it can be done, there is a risk that it will be and there will be things that you have not thought of.

Understand that it will go wrong. We are back to the woman with her knitted jumper. Knowing that the technology will go wrong at some point comes back to trust and confidence. If you otherwise enjoy the general trust and confidence of people, including elected representatives, you will be given the benefit of the doubt when it goes wrong and there will not need to be a review to say, "This is a systemic failing in the whole thing". If you have not and do not enjoy that trust and confidence, you are more likely to have some significant pushback against individual cases where it goes wrong.

There is a need to learn from the experience of where we got it right. Look at some aspects of technology that were very controversial at the time. Human fertility and embryology have been mentioned. BAC calculation and intoximeters were real changes for safe road use and countering drink driving. DNA is probably the most compelling example. I would go back to Lord Steyn's judgment in 2004 in S and Marper, which is where we started from, and the protection of freedoms. It said that it is of paramount importance that law enforcement agencies can access the latest techniques from modern technology, but it has to be in such a way that it is accountable, has independent oversight, is challengeable, is legitimate and everyone understands the risks, not just those trying to persuade someone of the procurement case to buy the kit and then try it.

Everybody needs to understand the issues, as I have found when I have been to Northern Ireland to cover my responsibilities there. If you are in a room with PSNI officers, you are in a room of people who understand human rights because they grew up with them. At the most recent meeting I had in Belfast, the superintendent said at the end, "I bet you've never heard so many police officers mention human rights as in this two-hour meeting". Culturally, that is really powerful and important.

Chair: That is because of the Good Friday agreement.

Baroness Kennedy of The Shaws: It is also true in the Army. Often, at high levels in the Army, you will find people very fluent on their obligations under human rights and international conventions.

Q18 **Lord Dholakia:** Have you discussed the use of artificial intelligence by police and crime commissioners in local areas? Do the inspectors of constabulary look at the monitoring of this scheme wherever it is adopted?

Professor Fraser Sampson: I have not discussed it with police and crime commissioners to any great extent. One, when I visited Avon and Somerset, had an interest in it. I do not think the police inspectors cover it. They have certainly never discussed it with me.

One thing that is telling from my recent survey of policing in England and Wales on the use of surveillance technology is the answers to question 112. When asked, "Who holds you to account for your use of biometric surveillance?", only four forces of the 39 respondents mentioned their police and crime commissioner. Given that nobody else is empowered to hold the police to account in England and Wales, I found that quite surprising really.

Lord Alton of Liverpool: Pursuant to what Lord Dholakia just asked about AI, given the Government's forthcoming White Paper, what should their priorities be?

Professor Fraser Sampson: Of all the questions now that I have been asked, for that one I might say that I do not know. They need to get the widest possible range of views from people who know what they are talking about, have lived through things going wrong and can sensibly, with an evidence base, predict what may go wrong. It is also about bringing them back to understanding that, by and large, there are areas where I agree with the aphorism that, "Just because we can doesn't mean that we should", but I go back and qualify that with the Article 3 point: that if you are the police or the state, there are some areas now where, just because you can, it might mean that you should, actually.

Chair: That is because of the positive obligation to use the means that are available to protect life under Article 2 and, looking back to the Worboys case, to investigate crime properly.

Professor Fraser Sampson: I was thinking of DSD, exactly.

Chair: On that last question about what the Government's priorities should be in the AI White Paper, I think it would be fair for this committee to conclude from what you said earlier that safeguarding human rights should be a high priority.

Professor Fraser Sampson: It should probably be the highest.

Chair: That is a pretty good note to end on.

Baroness Lawrence of Clarendon: How many people are in your team?

Professor Fraser Sampson: There is pretty well half of it behind me. There are seven and they are provided by the Home Office.

Chair: We are very grateful to you. That has been a very thorough and interesting session. You have given us a lot of material to think about and take forward in our role of scrutiny, so thank you very much, Professor.