OFFICIAL REPORT
AITHISG OIFIGEIL

Criminal Justice Committee

Wednesday 15 June 2022

Session 6

The Scottish Parliament
Pàrlamaid na h-Alba

Wednesday 15 June 2022

CONTENTS

CRIMINAL JUSTICE COMMITTEE
20th Meeting 2022, Session 6

CONVENER

*Audrey Nicoll (Aberdeen South and North Kincardine) (SNP)

DEPUTY CONVENER

*Russell Findlay (West Scotland) (Con)

COMMITTEE MEMBERS

*Katy Clark (West Scotland) (Lab)
*Jamie Greene (West Scotland) (Con)
*Fulton MacGregor (Coatbridge and Chryston) (SNP)
*Rona Mackay (Strathkelvin and Bearsden) (SNP)
*Pauline McNeill (Glasgow) (Lab)
*Collette Stevenson (East Kilbride) (SNP)

*attended

THE FOLLOWING ALSO PARTICIPATED:

Dr Brian Plastow (Scottish Biometrics Commissioner)

CLERK TO THE COMMITTEE

Stephen Imrie

LOCATION

The David Livingstone Room (CR6)

Scottish Parliament

Criminal Justice Committee

Wednesday 15 June 2022

[The Convener opened the meeting at 10:00]

Decision on Taking Business in Private

The Convener (Audrey Nicoll): Good morning, and welcome to the 20th meeting in 2022 of the Criminal Justice Committee. No apologies have been received.

Under agenda item 1, do we agree to take items 3, 4 and 5 in private?

Members *indicated agreement.*

Scottish Biometrics Commissioner: Draft Code of Practice

10:00

The Convener: I am pleased to welcome Dr Brian Plastow, in his first appearance before us as Scottish Biometrics Commissioner, to talk about his first draft code of practice on the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes in Scotland. I refer members to papers 1 and 2 and I invite Dr Plastow to make some opening remarks.

Dr Brian Plastow (Scottish Biometrics Commissioner): Good morning, and many thanks for the opportunity to speak to you about the draft code of practice that we have produced, as the convener said, to address the acquisition, retention, use and destruction of biometric data for policing and criminal justice purposes in Scotland.

As committee members will be aware, the Parliament passed the Scottish Biometrics Commissioner Bill in 2020, in the previous session. The bill received royal assent on 20 April 2020 and I was appointed as commissioner a year later, on 12 April 2021. My first task was to build the new function from the ground up, and I am pleased to inform the committee that that work is complete.

In my role as commissioner, I have three main functions. The first is to support and promote the adoption of lawful, effective and ethical practices on biometric data and technologies for policing and criminal justice purposes in Scotland, specifically by Police Scotland, the Scottish Police Authority and the Police Investigations and Review Commissioner; the second is to promote public awareness and confidence around such matters; and the third is to develop the code of practice. How I intend to do all of that was set out in my first strategic plan, which was laid before the Parliament on 24 November 2021.

As members will be aware, section 7 of the Scottish Biometrics Commissioner Act 2020 requires me to prepare a code of practice, section 10 lists those whom I must consult in preparing the draft of that code, and section 11 deals with procedural matters in securing ministerial consent to lay a draft before the Parliament. We are at that stage now, and I will say briefly how we got to this point.

The first draft of the code, version 0.1, was developed around July last year, and it went to my professional advisory group, which I am required to maintain under section 33 of the 2020 act. The

membership of that group can be found on page 54 of the draft code.

After a few amendments, version 0.2 was the subject of a three-month closed consultation, which ran from October to December 2021 and involved consulting around 33 or 34 individuals, office holders and groups. They included the 12 that are prescribed in the act, and the remainder were others whom I regard as significant stakeholders in the field. At that point, I also wrote to the Cabinet Secretary for Justice and Veterans and to this committee.

That led to the production of version 0.3, which was presented to the cabinet secretary and Government officials in January. We then received the cabinet secretary's consent to lay before the Parliament version 0.4, which you now have. At the same time, we placed that version on our public website to facilitate a level of public consultation and engagement on the product.

My message to the committee is that the version that you now have is the product of a thoughtful and well-considered consultation. It has the unequivocal support of those who were consulted, including those to whom it will apply.

The code is constructed with what I call lead-in material, compliance factors and lead-out material. Everything up to page 26 is the lead-in material. It explains the purpose of the code, the distinct meaning of "biometric data" in Scottish legislation, the main biometric databases in Scotland, and our distinct legal framework. That is important because, although the police across the United Kingdom share common biometric databases, the data that goes into them comes from very different jurisdictions and is defined differently in different contexts.

The main meat of the code, if we want to call it that, is on pages 27 to 35. It revolves around 12 general principles and ethical considerations that must be followed to ensure compliance with the code. The guidance also forms both a self-assessment framework and a guide to professional decision making for those to whom it will apply.

I describe the remainder of the code as the lead-out material. It explains what would happen if there was non-compliance with the code and the mechanism for public complaints if a data subject feels that one of the bodies is not compliant. There are appendices to help readers to understand what that is all about.

The primary audience for the code is made up of Police Scotland, the Scottish Police Authority and the PIRC. Once the code is approved, we will produce a short, user-friendly, public-facing version.

It is important to draw the committee's attention to the fact that, in all the consultation that we have conducted so far, there have been no dissenting voices on either the content of the code or its principles-based approach. In my professional opinion, that is because it has been a well-considered piece of work that has been developed with partners across the criminal justice community. It strikes the right balance between allowing the police the means to do what they need to do to keep everyone safe and protecting the individual human rights of members of the public while factoring in privacy and ethical considerations.

I am looking for the Criminal Justice Committee's support to get to the next stage, which will be to put a final draft to Scottish ministers so that they can lay a statutory instrument in due course to bring the code into effect. When it is introduced by regulation, Scotland will become the first country in the world to have a statutory code of practice for the acquisition, retention, use and destruction of biometric data for criminal justice and policing purposes. That will be a significant human rights achievement for Scotland and something that we should be proud of. It will further help to enhance confidence in Scotland's already excellent criminal justice system.

I am happy to take questions.

The Convener: Thank you, Dr Plastow. That was a very helpful overview of and introduction to the code of practice in its current form.

You said that the meat of the draft code of practice is structured around 12 guiding principles and ethical considerations to which Police Scotland, the PIRC and the SPA must adhere when they acquire, retain, use or destroy biometric data. Will you expand on how those principles and considerations were developed and how they were identified as being appropriate to the code of practice?

Dr Plastow: I am happy to do that. I should start by explaining my journey. As committee members will know, I was a police officer for more than 30 years, and I was a chief superintendent for my last five years. The issue was first raised in the Scottish Parliament by Alison McInnes back in 2015. It had been identified by the Commissioner for the Retention and Use of Biometric Material for England and Wales at the time, the police service in the UK having rolled out facial search functionality to the UK police national database. I was working at Her Majesty's Inspectorate of Constabulary in Scotland at the time, and I was asked to do an audit and assurance review of how Police Scotland was using the new facial search functionality. It is a retrospective tool.

During that review, we examined the whole landscape around biometric data in Scotland. That took us back to the Fraser report from 2008, which had identified the issue that there was no independent oversight in Scotland in relation to this landscape. That projected forward into the new landscape following the police reform. Police Scotland and the Scottish Police Authority jointly operate the main DNA and fingerprint databases, which precludes the Scottish Police Authority from marking its own homework, if that is not too crude a way to describe it.

Subsequently, in 2017-18, I was invited on to the independent advisory group on biometric data in Scotland that was chaired by John Scott QC. I was invited on to the group as a subject expert to help John Scott to produce his report to the Parliament. He was very keen on a principles-based approach. We did a lot of academic research and we looked globally to see what direction other countries were taking in the area. We arrived at a principles-based approach that was built not only on the work of the independent advisory group, but on the approach that was being taken globally. In the UK context, the Home Office's Biometrics and Forensics Ethics Group operates to a principles-based framework. The Biometrics Institute, which is a global organisation that promotes the responsible use of biometrics, also operates to such a framework.

There is a distinction between what the law needs to do in setting hard-and-fast rules and what a code of practice can achieve by providing a framework for ethical decision making.

Does that answer your question?

The Convener: Yes. That is very helpful. It gives us a context and the backdrop to how the principles were developed.

It is fine to have principles and ethical considerations in the code of practice, but I am interested in how compliance with the code will be monitored in future. For instance, will there be a continual monitoring and reporting process with the relevant policing bodies, or is there another process that you feel will work best for the monitoring role?

Dr Plastow: I have a three-part answer to that question. First, my intention is that, from a year after the code is brought into effect under regulations, there will be an annual compliance assessment for each organisation to which the code applies. If we use Police Scotland as an example, that will be predicated partly on the police being issued with a self-assessment questionnaire based on the national assessment framework, which can be found in one of the appendices at the rear of the code. That framework contains 42 quality indicators, as we call them—in other words, indicators of what "good" looks like. I will pick a selection of questions from that framework and ask each organisation to carry out a self-evaluation, which will be followed by some fieldwork to validate and confirm that what we have been told is correct.

10:15

Another strand of the process is the rolling programme of thematic reviews in the strategic plan. For example, towards the end of the year, we will look at how biometric data on children and young people is being acquired, retained, used and destroyed, as part of the bigger agenda in that respect. In subsequent years, we will look at fingerprints, DNA and so on.

The third strand is the on-going review. I mentioned the professional advisory group that has been established under section 33 of the 2020 act, which includes the bodies to which our functions extend. At its meetings, there are opportunities to discuss emerging trends and pertinent issues. I also have very regular, on-going meetings with Police Scotland, the PIRC, the Scottish Police Authority and even bodies to which my functions do not currently extend, such as the National Crime Agency, the British Transport Police and the Ministry of Defence Police, which also operate in Scotland.

In short, our approach has three strands, but there is also a programme of annual compliance assessments.

The Convener: Thank you for that really interesting response.

I open the questioning up to other committee members, starting with Katy Clark.

Katy Clark (West Scotland) (Lab): Thank you for your comprehensive introduction, commissioner, which addressed some of the issues that I was going to ask about. You gave us an explanation of the lead-up to the creation of the draft code of practice and the consultation process, and it sounds as though there was a high level of consensus in the discussions on what should be in the code. Were there any contentious issues? What might be the contentious issues for the public? Did you think that any issues might be contentious before you had the discussions, even if it turned out that there was consensus among those who were involved?

Dr Plastow: Again, I will have to give a multipart answer to your question. First, in the process of arriving at version 0.4 of the draft code of practice, there was a high level of consensus on the 12 general principles and ethical considerations, which were identified as being the right ones, but there was also a lot of debate and discussion

about what should be in each of them. I had some fantastic input from the UK Information Commissioner's Office, the Scottish Human Rights Commission, equality organisations and others including Police Scotland. The general principles have evolved and expanded to include additional information and hyperlinks that signpost readers and users of the code to other relevant guidance such as the Information Commissioner's Office guidance on data protection, equality and human rights guidance, et cetera.

As for whether anything surprised me, an issue arose that is not just to do with the code. To tie in with my function of helping to promote public awareness, understanding and so on, we commissioned ScotCen Social Research back in December to carry out a public attitudes and awareness survey for us, because we thought that it might be useful to try to baseline that. A sample of 1,154 people were asked eight questions to test what they knew and thought about the use of biometrics for policing and criminal justice purposes.

The eighth question was on live facial recognition. As the committee will know, Police Scotland does not use that and it has never been deployed in Scotland. I expected the people in the sample to be strongly opposed to it, but they were not. Of course, it was only a small sample, but that illustrates the fact that we do not know anything until we engage with people and ask for their opinions. A lot of the optics on this stuff has come through the lens of the media, and it is important that we know what the public know and feel and where their boundaries of acceptability lie.

I am sorry—did I miss the point of your question?

Katy Clark: No. Your response is really helpful. I suppose that that highlights some of the issues with the technology. If people thought that it was 100 per cent accurate, they might be comfortable with it, but the risks of it going wrong will always be an issue.

You talked about keeping the process under review through annual compliance assessments. How will you ensure that the process is robust, that you really engage and that you hear the difficult voices and not just those of the people who are already part of the system?

Dr Plastow: First, I want to get it out there that there is no such thing as a completely accurate biometric system, because the systems rely on interactions between humans and technologies. Some systems are better than others.

The answer to your question is about knowing which questions to ask. Because I come from the policing world and I have an intimate understanding of police databases—for example, where they are kept and what they contain—I know the right questions to ask. It would be difficult for someone who does not have the subject knowledge or expertise to ask the right questions. I assure the committee that I will be asking the right questions and that, when I do so, those to whom I direct them will know that I probably know the answers to the questions that I am asking—if that helps.

The Convener: Did you want to come in here, Jamie?

Jamie Greene (West Scotland) (Con): Yes. It is not necessarily on the same issue, but it follows on.

Good morning, commissioner. I have to say that I find this quite challenging. As you have said, much of the narrative being played out in the media is about a polarised debate between human rights and public safety considerations and the use of technology that enforcement agencies could and should be using.

If the SPA or ministers were to propose, say, a trial of facial search or recognition technology at a specific event or locus or just some wider policy, what test would you subject it to? Would it simply be subject to the code of practice? At what point would you feel comfortable with pushing back on political decisions or even operational matters being proposed by the police or ministers and saying, "No, I'm uncomfortable with this"?

Dr Plastow: Thank you for that interesting question. It is not my role to interfere with the operational independence of the chief constable. However, because of the mature relationship that I already enjoy with the bodies to which my functions extend, if they wished to pilot a new technology in the circumstances that you have described, I hope that they might want to involve my office in evaluating it.

I suppose that the hot topic is facial recognition. Police Scotland uses only two types of retrospective facial recognition. The police national database, which is a UK-wide intelligence sharing system, has a retrospective facial search capacity.

Basically, you can upload an image from a crime scene—a probe image—to the police national database. That image will then be compared against a gallery of images derived from previous custody episodes. Depending on the quality of the probe and gallery image, the system might bring back a shortlist of 30 potential matches, which a human being then needs to look at to decide whether it could be the same person. There is also a retrospective facial search capability in the child abuse image database. Police Scotland does not use any other form of facial recognition, either in the overt world, which would fall within my jurisdiction, or the covert

world, which would fall within the Investigatory Powers Commissioner's jurisdiction.

However, let us say that Police Scotland decided that it wanted to introduce live facial recognition technology and apply it to body-worn video cameras in specific scenarios such as firearms operations and so on. I would not be opposed to that as a concept. The questions would be around lawful basis, proportionality and necessity, whether the technology works and does what it says on the tin, and whether the algorithms are free from bias or discrimination.

I am your commissioner, but I am also their commissioner. If Police Scotland, the Scottish Police Authority or the Police Investigations and Review Commissioner wanted to use my office to help them get to a place that they need to get to in a safe way that reassures the public, I would hope that they would have the confidence to do that.

Jamie Greene: That is helpful. The scenario that you mentioned is a useful one to put the issue in context, but there are obviously hundreds of other scenarios. My concern is about how you worded and structured your answer, in that it seemed to imply that it would be nice if they involved you, but that there is no statutory duty on them to do so. Theoretically, I guess that that means that they could do what they want in that respect within the confines of what is and is not legal—in the overt environment, anyway; we know what happens in the other world. If they did not actively involve you, you would therefore be merely an observer to the proceedings and then part of the mop-up in deciding whether any good or damage was done. Does that make you feel uncomfortable? Would you prefer a more active or statutorily powerful role?

Dr Plastow: It does not make me feel uncomfortable because, in the same way that I have a good level of confidence in Police Scotland, I would hope that it would have the same level of confidence in me through the professional working relationship that we have. I could pick up the phone to the chief constable tomorrow; I have that relationship with them because we have known each other for many years.

In answer to the other point, yes, there are gaps in the legislation. One of the issues is that there are different definitions in the UK of what constitutes biometric data. There is the Scottish definition, which is an all-encompassing and very good definition, and the England and Wales definition under the Protection of Freedoms Act 2012, which extends only to fingerprints and DNA. That becomes relevant when we think of my counterpart in England and Wales, Professor Fraser Sampson, with whom I have an excellent working relationship.

Fraser is responsible for reviewing national security determinations, which means that if biometric data was retained in Scotland under a national security determination, it would fall to Fraser and not myself. However, the 2012 act that enables him to do that covers only DNA and fingerprints, and it is inconceivable that, if the police were retaining somebody's fingerprints and DNA, they would not also be retaining their other biometric data. The question is therefore: who exercises oversight over that? There are gaps in the legislation and it is not perfect, but we often operate in cluttered landscapes.

When the proposal to create a Scottish Biometrics Commissioner was first made way back in 2015, the thinking and fundamental argument was that the police were minority holders of biometric data in Scotland and the UK. In fact, local authorities and health boards hold most biometric data. Although the original thinking—probably three cabinet secretaries ago—was therefore that the role would be more all-encompassing, the decision was taken that it would be restricted to the criminal justice portfolio.

10:30

Jamie Greene: The reality is that our phones have more biometric data about us than the police, local authorities or the NHS. The problem is that we are talking about narrow use of facial recognition, such as cameras that identify people at football matches, but if we look at where technology has gone, it is 100 years ahead of that. There is ear recognition, hand and finger recognition and vein pattern and voice recognition. Artificial intelligence could be using pretty much everything about you to proactively identify you, and it is already happening in many commercial settings. However, we are talking about what happens in the legal world and we already know that law enforcement agencies in some countries are using it to discriminate and pull out certain ethnic and minority groups to incarcerate them. It can therefore do down a dangerous road. Thankfully, we do not live in that environment.

The Convener: There is a lot of interest in this particular line of questioning. I will bring in Russell Findlay and then Pauline McNeill.

Russell Findlay (West Scotland) (Con): Good morning. I think that you have answered one of the questions on my list, which was about the difference between yourself and the biometrics commissioner down south, which has been in existence since 2016. You have a much broader scope of material or factors to consider. Is that general assessment correct?

Dr Plastow: Yes. If we rewind on all that, England and Wales used to have a biometrics

commissioner, a separate surveillance camera commissioner and a separate forensic science regulator. Scotland had none of those things. When the role of the Scottish Biometrics Commissioner was created, by including source samples in the definition, an attempt was made to close the gap a little bit in relation to the forensic science piece.

The role that Fraser Sampson now performs in England in relation to biometrics and surveillance cameras was rolled into one new role. He has two offices, one of which relates to public space surveillance cameras and another that specifically relates to fingerprints and DNA. He therefore has a bigger portfolio in terms of geography, but the definition of biometrics in Scotland is far more extensive.

Russell Findlay: One bit of information in a briefing that we received suggests that the Scottish Government was seeking that biometric data held by UK policing organisations, such as the British Transport Police, the Ministry of Defence Police and the NCA, should come within the remit of the Scottish Biometrics Commissioner. Has that happened?

Dr Plastow: No. It is a long and drawn-out process but, basically, Scottish Government officials are pursuing a section 104 order under the Scotland Act 1998 to try to extend the functions of the Scottish Biometrics Commissioner to include those three policing organisations in relation to their Scottish operations. Obviously, it is in the gift of the Westminster Parliament to approve that, but in preparation for that I included the National Crime Agency, the British Transport Police and the Ministry of Defence Police in the consultation when drafting the code of practice. All the chief officers wrote back favourably and indicated that, if that section 104 order is granted, they would be more than happy to come under the auspices of my office and code of practice, and that they would also welcome the opportunity to come on to the professional advisory group. The support is therefore there; the challenge is in getting it across the line.

The committee might also be aware that the Department for Digital, Culture, Media and Sport in England and Wales launched a consultation last year whereby it is, in effect, trying to give the functions of the commissioner for England and Wales to a newly constituted Information Commissioner's Office. In other words, it is trying to reduce all the complexity around police use of biometric data to a question of data protection, but the issue is far greater than that. In response to that consultation, although it covered England and Wales only, we wrote a joint letter with Professor Fraser Sampson not only to UK ministers but to Scottish ministers to highlight why that was not a good idea.

Russell Findlay: These organisations operate UK-wide. Was any consideration given to including the security services?

Dr Plastow: That would be a question for the Scottish Government rather than me. I am not driving the section 104 order request—that aspect is being driven by Scottish Government officials as a result of the quite legitimate concerns that members of the Scottish Parliament raised during the passage of the bill that became the 2020 act. I understand fully why you are asking that question—the security services obviously hold biometric data.

Pauline McNeill (Glasgow) (Lab): I have a supplementary question about something that Dr Plastow said earlier.

It surprised me when you said that local authorities hold most of the biometric data; that was news to me, I have to say. I am sure that the answer is obvious—maybe it relates to the delivery of services—but could you expand on why that would be?

Dr Plastow: I go back to the point that Jamie Greene made when he held up his phone. To answer your question directly, local authorities hold a lot of people's individual biometric data, such as photographs and so on, as do the national health service, public space surveillance cameras and the automatic number plate recognition system. There is quite a big "surveillance landscape"—in inverted commas—out there.

It is interesting to reflect on the past 12 months, which was my first year in office. Have there been any scandals or controversies in relation to the use of biometric data in Scotland by Police Scotland, the Scottish Police Authority or the PIRC? The answer is no. Have there been any controversies in other contexts? Yes, there have. The first was around the debate on the use of facial recognition technologies in schools in North Ayrshire as a means of administering school meals. The second was when the UK Information Commissioner publicly reprimanded NHS Scotland and the Scottish Government for failing to protect data within the Covid certification apps. That was about allowing the supplier of the algorithm to retain people's facial images for five days to test its software.

I am trying to highlight to the committee that policing and criminal justice are minority users of such data. Another good way to look at it is by looking at the Home Office biometrics programme, which is a big programme to join up the biometric databases of policing, immigration and other central Government services. There are currently 120 million biometric records relating to 85 million

people in the Home Office biometrics programme, but only 26 per cent of that data is police data. There is an awful lot of this stuff out there.

Why that is important for Scotland is that Scotland needs to ensure that when it contributes Scottish data to national policing systems, it retains control of that data. In addition, it is not just a question of what data Police Scotland, the PIRC and the SPA hold. It is also a question of what data they can access when using the national systems.

The age of criminal responsibility in Scotland is now 12, but it is still 10 in England and Wales. The police in England and Wales retain images of people on the police national database who have never been charged or convicted of any offence. Police Scotland does not do that, but it can access the images that are on the system.

The subject is inherently complicated. I am just trying to get over the message that biometric data is everywhere, and policing is actually a minority player in some of it.

Pauline McNeill: On the question of surveillance that comes under local authorities, is it part of your role to ensure that those surveillance systems are not being abused? Who checks that?

When you were talking just now, I thought you were going to mention that, certainly in England, local authorities have been using surveillance to try to catch parents out in relation to school catchment areas. That seems to cross a line in some respects. I do not think that it has happened in Scotland.

Dr Plastow: To answer your question, Scotland does not have a surveillance camera commissioner—that is not part of my role. The UK Information Commissioner has a distinct locus in relation to biometric data, which, under article 4(14) of the UK general data protection regulation, is defined as data that arises "from specific technical processing".

We can think of town centre closed-circuit television, for example, which captures people's images but does not use them—the system typically overwrites after 30 days. That would not be classed as biometric data under the UK GDPR. Where it becomes biometric data is where an image is taken and attached to the profile of an individual.

The answer to your question is that, from a data protection perspective, the ICO is the only organisation that looks at public space surveillance. It undertakes enforcement activity, and it has done so in the past. However, with regard to broader questions of legitimacy, effectiveness and ethical considerations, there is not a specific office, like the role that Fraser Sampson performs in England and Wales, that looks at that area in Scotland.

Rona Mackay (Strathkelvin and Bearsden) (SNP): Good morning, Dr Plastow. I want to pick up on the thread that Jamie Greene and Pauline McNeill have been following, but I also have another question on a different subject.

My first question relates to facial recognition. My colleague Fulton MacGregor will back me up here but, in the previous parliamentary session, the Justice Sub-Committee on Policing took a lot of evidence on facial recognition, particularly with regard to its accuracy. There were, for example, problems with the software recognising people from ethnic backgrounds.

However, I am now a bit confused. Can you clarify your comment to Jamie Greene about the police using retrospective images from previous custodies and so on? Was the new technology, on which the sub-committee took a lot of evidence, just never implemented? Are the police using it or not?

Dr Plastow: I will outline what the issue was all about. What kicked it off was that, when Police Scotland originally published its policing 2026 strategy, it contained a statement that it was going to roll out live facial recognition. Of course, when the former Justice Sub-Committee on Policing looked at some related issues—specifically, the use of digital triage devices, digital forensics and so on—the whole piece came to the political fore. For the avoidance of doubt, Police Scotland has not used live facial recognition in Scotland, ever, and especially not in the way that we have seen it used down south, for example, at rugby matches or at the Notting Hill carnival.

It might help committee members to understand the distinction between biometrics that establish characteristics of uniqueness versus those that establish only similarity. Let me take, as an example, DNA. Other than identical twins, nobody has the same DNA. That means that, when a DNA profile is analysed, if it is of sufficient quality and quantity, the probability of someone being misidentified is less than one in a billion. It is similar with fingerprints. Because fingerprints are formed on an embryo's little hands by environmental factors as the baby moves around in the womb, no two individuals on the planet—not even identical twins—have ever been found to have identical ones.

10:45

Both of those sciences—and they are sciences—deal with the characteristics of uniqueness; however, our faces are not unique. Humans have evolved into being very good at identifying faces, because it helps us to know

where our mums, dads, uncles and friends are. However, machines are really bad at it. That is why a traditional police mug shot is taken with the subject in a certain position. It is also why, when you apply for a UK passport, you are not allowed to smile or to wear sunglasses.

No technology that deals with faces is as reliable as any that deals with fingerprints or with DNA, because it looks for characteristics of similarity. I have given examples of the police's use of retrospective facial search in the police national database and the child abuse image database. They use a machine to try to reduce a huge sample of hundreds of thousands of images to a shortlist of perhaps 30 that a human can look at and say, "That could be him." Facial recognition is not at all a reliable technology.

Rona Mackay: Are you saying that Police Scotland has not used live facial recognition technology?

Dr Plastow: That is correct.

Rona Mackay: Is that an operational decision? Does Police Scotland have the capacity to do that, or have the police just decided not to?

Dr Plastow: Police Scotland was asked to give the previous Parliament reassurance on that in response to concerns raised by the Justice Sub-Committee on Policing about a statement in Police Scotland's 10-year strategic plan. At that juncture, Police Scotland indicated that it had no plans to pursue that. I am not aware of any current plans to do so.

Rona Mackay: My next question is on something that I know that you have already talked about and which is in the code of practice, but I would like an answer to go on the record. Can you please set out, in broad terms, the specific legislation to which the code will apply?

Dr Plastow: The easiest way to answer that is by saying that it will apply to all criminal justice legislation in Scotland that is not already within the preserve of another UK Commissioner.

Because my functions do not extend to data protection per se, any specific complaint about a breach of the Data Protection Act 2018 would go to the Scottish Information Commissioner. My powers also do not extend to the relatively small numbers of biometric materials retained in Scotland under a national security determination—that is Professor Fraser Sampson's role. Finally, if a complaint about biometric data obtained through covert policing operations was made under the Regulation of Investigatory Powers (Scotland) Act 2000, that would have to go to the Investigatory Powers Commissioner.

Those are the three exceptions. I regard everything else as falling within my remit.

Rona Mackay: Thank you. Finally—and you might not be able to answer this question—have you had any indication of when to expect the code of practice to be approved by ministers?

Dr Plastow: I have discussed that with Scottish Government officials. Once I have had the committee's feedback, and any amendments that you might want are made, the drawing up of a Scottish statutory instrument will be relatively straightforward. The difficult part will be finding parliamentary time to introduce it, but my best guess is that we might be looking at the autumn.

That would work, because we have developed in parallel with the code an accompanying draft complaints procedure, which we are discussing with a number of bodies. After all, things could become complicated. For example, someone might make a complaint to me about a potential breach of the code of practice and then also complain about the same thing to the PIRC, and we have to ensure that processes and procedures are agreed between us so that there is no blue-on-blue activity.

Rona Mackay: Thank you—that was very helpful.

The Convener: Picking up on your comment that Police Scotland has indicated that it has no plans to introduce facial recognition at the moment, I note that you said that you are also the commissioner for Police Scotland. What would be your role if it changed its position on using or not using a specific biometric data collection method such as facial recognition? Would you have a role in supporting it, or is your role more about regulation?

Dr Plastow: The answer to that is twofold. My role under the legislation is

"to support and promote the adoption of lawful, effective and ethical practices".

The answer to your question lies in those three key words: "lawful", "effective" and "ethical".

Hypothetically, if Police Scotland identified a facial recognition technology that worked—which would be the first real challenge—and decided that it wanted to deploy it at, say, a Scotland v France rugby game, it would, notwithstanding the lawfulness question, be very difficult for it to demonstrate that such a move was proportionate and necessary in the absence of a specific threat against that event. On the other hand, if it had access to a technology that worked, was reliable and was free from bias and discrimination and if there were a G20 meeting or similar event in Scotland against which there was a specific intelligence threat from a number of known individuals, photographs of whom the police had access to, its use would be legitimate. However, I

would suggest that any such activity would happen covertly.

I have been accused of being anti-facial recognition—I am not. I have just said that I am opposed to the way in which it has been implemented in other jurisdictions. I would not be in favour of it if its use had been held to be unlawful, because community impact assessments or equality impact assessments had not been done, and if the technologies rolled out clearly did not work and contained discriminatory algorithms. Who would? In the Bridges case in south Wales, for example, it was ruled to be unlawful not because it was facial recognition but because the various impact assessments had not been done and reasonable steps had not been taken to ensure that the technology was not discriminatory.

The police in England and Wales are very much pressing ahead with the technology. Interestingly, they are citing common law as the lawful basis for its use. In other words, they are using laws that have evolved from medieval times as the lawful basis for mass public-space surveillance. I have some issues with that.

The Convener: Thanks very much. That was helpful.

Russell Findlay has a question on the voluntary provision of biometric data.

Russell Findlay: I just want quickly to touch on what is going on elsewhere in the United Kingdom. Dr Plastow, you have previously been quoted as describing what is happening there as a "dangerously authoritarian path". I do not know whether that relates specifically to the case in south Wales or is a more general comment, but it prompted a rebuke from the Scottish Police Federation, which went as far as to question your objectivity. Has that been resolved? Have you had conversations with the SPF? Does it now understand where you are coming from?

Dr Plastow: You will forgive me for saying so, but that was a misguided comment from the SPF. I have written to the federation before; I did so when I developed the first version of the code and the first version of the strategic plan, but I did not get a response.

I received a request from a journalist from *1919* magazine, which is funded by the federation. When, during the interview, I was asked for my views on live facial recognition, I said that it did not happen in Scotland, and I gave a view on how it had been used in two specific scenarios in England. One was its use at the Notting Hill carnival, where the technology at that time was found to be something like 90 per cent inaccurate; in other words, nine out of 10 people were misidentified. In that case, the London Policing Ethics Panel had a look at it afterwards and found that there had been no equality impact assessment or consideration given to the impact that it would have on the black and minority ethnic community.

In the Bridges case, I was simply citing a matter of fact, which was that the UK High Court or Supreme Court—whichever it was—ruled that the way in which technology had been deployed was unlawful. It was not unlawful because of its deployment but because of the lack of impact assessments and the failure on the part of South Wales Police to satisfy itself that the technology did not operate on the basis of discriminatory algorithms.

I think that my remarks were interpreted out of context by someone who could easily have picked up the phone to speak to me but chose not to. I have tremendous respect for the Scottish Police Federation, and the comment was like water off a duck's back for me. It came from just one individual office holder.

Russell Findlay: Your four-year plan talks about your first annual report to Parliament being due in summer 2022. Do you have a date for that?

Dr Plastow: My first annual report is written. However, as the committee might or might not be aware, you have to go through quite a bureaucratic process to land an annual report. Even though I am a tiny organisation with only three members of staff, I still have to go through the full Audit Scotland financial and performance audit. That is happening at the moment. Because of the way in which that works, until my accounts are signed off by the Auditor General—and the window for that is September—my report, even though it is written, will probably not see the light of day until October.

As I have said, the annual report is written. It would be wrong to say what is in it in its entirety, but the key message that I would leave with the Criminal Justice Committee is that, in my view and at this moment in time, the Parliament should have confidence in the way in which biometric data is being used for criminal justice and policing purposes in Scotland.

Russell Findlay: I presume that the annual report will also address where you are at with each of the 15 key performance indicators.

Dr Plastow: A legislative anomaly has arisen in that respect. When the original legislation was passed, my financial and reporting periods were aligned in law, but because the pandemic caused a delay in recruiting a commissioner, a Scottish statutory instrument was subsequently laid that misaligned in law the period of my strategic plan and the period of my finances. My finances therefore run conventionally from April to April

while my strategic plan runs from December to November.

I intend to put a recommendation in my first annual report about that. I have asked Scottish Government officials about it, and we need to find a way of returning to the original plan, as I am the only independent office holder in Scotland whose financial and reporting periods are misaligned in law. That does not help me, it does not help the committee and it does not help Audit Scotland, so I hope that, by including the recommendation in my report, the issue can be addressed at a convenient opportunity.

Russell Findlay: And it happened because of Covid.

Dr Plastow: My understanding is that, given that the legislation was passed in April 2020 and the process to start recruiting a commissioner started in December 2020, it was a Covid consequential.

The Convener: I call Katy Clark.

Katy Clark: I was not going to come in on this issue, convener.

The Convener: In that case, I call Collette Stevenson.

11:00

Collette Stevenson (East Kilbride) (SNP): Good morning, commissioner. You have touched on the significant legal and ethical issues in relation to the different uses of biometrics that have been highlighted in the code of practice. Will you talk about some of the work that will be undertaken on assessing legal and ethical issues in relation to emerging technologies?

Dr Plastow: The idea of a code of practice arose, as it often does in other contexts, because the law is a blunt instrument. It takes a long time to change the law and, by the time that that is done, technologies have already made a quantum leap into the future. I think that that point was made earlier on. The idea of having a code of practice in the first place is that it is more fleet of foot, it can be kept under review, and it can be adapted and amended on a regular basis.

Ethical considerations are everywhere. I originally entered the world of policing in 1978. DNA profiling had not been invented, and nobody had heard about it. At that time, the police took fingerprints by taking a tube of ink, putting some ink on a brass plate, and rolling it out. Basically, you got the prisoner and yourself covered in ink. Photographs were taken with the latest Kodak camera. Things have moved on quickly—in the past 20 years, scientists have sequenced the entire human genome.

One thing that I will highlight in my annual report, which members will see eventually, is that Scotland already operates at a higher level of DNA interpretation and analysis than the rest of the UK does. The UK and Europe use DNA-17 profiling; Scotland uses DNA-24 profiling. For the past 20 years, it has been possible to sequence the entire human genome, but should we use that technology? Just because the police and others could use DNA to identify the skin colour or eye colour of a sample that was retrieved at a crime scene, should they use it?

Such ethical debates, particularly on DNA, are at the heart of the whole piece around live facial recognition. Is it appropriate in a modern democratic society for citizens to unknowingly be subject to mass public space surveillance—yes or no? Regardless of whether there is a basis in law, is that ethical, proportionate or necessary? Could we achieve the same results with traditional policing methods?

It really is fascinating stuff and, as with many things in life, there are no right and wrong answers. I am proud of the way that Scotland has led the way on the issue through the policy framework and the more all-encompassing definition of biometric data, because that says something about the sort of society that we want to be and that we want to live in.

The point about what will happen if we get this stuff wrong has been made well by members. Look at how things are used in China to suppress Uyghur Muslims. China and Russia hold the two biggest state biometric databases in the world. It is not my role to comment on how they use that data, other than to say that they do.

The UK holds enormous amounts of biometric data. As the committee might be aware, the European Union is in the process of rolling out a massive facial recognition database under Prüm II. For anyone who has never been there, Prüm is a small town in Germany. The existing arrangements named after it cover the exchange of biometric data, fingerprints and DNA between the UK and EU member states, subject to controlled conditions. At the moment, those do not extend to facial recognition data, but the European Union clearly wants that to happen. I suspect that the UK Government will, too.

I have probably gone off on a tangent there—that is a pet subject of mine.

Collette Stevenson: No, not at all. It is all fascinating stuff.

You touched on your annual report, which ties in to our discussion. Who oversees the procuring of all those technologies? You mentioned local authorities, and we have also heard that only 26 per cent of biometric data in Scotland is held by

Police Scotland. Do you have any input into the procurement process?

Dr Plastow: Yes and no. That is a good question.

In relation to fingerprints and DNA, the UK national database—I am sorry; let me go back a stage. Scotland has its own DNA database, from which Scottish samples are uploaded to the UK national DNA database. Scotland does not have a fingerprint database; whether it should have is another question. Scotland uses the UK fingerprint database, which is known as IDENT1. Scotland also has lots of databases that contain facial images. However, the only ones that are uploaded to the UK system in biometric terms are from Police Scotland's criminal history system, from where pictures of people who have been arrested and charged go into the police national database, or PND.

I sit on the strategy board of the UK-wide forensic information databases service—FINDS—which is a strategic group, chaired by a deputy chief constable, that oversees the management of the UK fingerprint and DNA databases. I do not have a seat on the National Police Chiefs Council group that oversees police use of facial images, and neither does my counterpart in England and Wales, because facial images do not fall within his remit.

That is a roundabout way of saying that I am very confident in what is happening on fingerprints and DNA, but far less so on what is happening on national approaches to facial recognition. The DNA and fingerprints databases are procured and approved by the Home Office to ensure that, among other things, there are no discriminatory algorithms. The police tend to do their own thing on the facial aspect, so I cannot comment on that. The PND, which Police Scotland uses, is a Home Office-procured system. We have seen from the media that other systems that have been used by forces down south have perhaps been let out of the box too soon. However, we are where we are with that.

Collette Stevenson: Thanks very much. That is really helpful.

The Convener: Apologies for my conferring with the clerk. I am just ensuring that I bring everyone in and that we cover as many themes as we can.

Would Jamie Greene like to come in at this point?

Jamie Greene: Yes. My question follows on nicely from the point about procurement. It is not directly about that, although procurement is an issue.

I am sure that you will remember that, as far back as 2015, through the future cities project, Glasgow procured a high volume of digital surveillance cameras to replace its old analogue system, at a cost of around £24 million. Around 500 cameras currently sit there. They are capable of providing forms of facial identification if the appropriate software were to be enabled. That was quite widely reported at the time and probably quite widely resisted by many stakeholders.

Reading between the lines, it seems that the Scottish Police Federation is of the view that its operational members in front-line policing are very much in favour of much more enhanced use of technology on a proactive basis, such as the enabling of CCTV to perform certain functions around the specific targeting of people, tracking missing persons and preventing crime in certain areas of the city. However, off the back of the 60-page report that the Justice Sub-Committee on Policing published in the previous parliamentary session, the federation felt that those views had not been taken fairly into account by that sub-committee. I say that with respect to members of the current committee who sat on the sub-committee. That is just a general overview on the part of the federation.

It seems to me that there is a conflict. It seems that local authorities and operational police are very much in favour of the benefits of the technology, but they feel that its use has been thwarted by a public or political perception of the so-called big brother state argument. Where do you sit on that? Are you likely to make a more proactive recommendation to Glasgow City Council and the police on enhanced use—in other words, the switching on—of those cameras, which are sitting there and not being used to their benefit?

Dr Plastow: That is an interesting two-part question. I will put the Glasgow City Council aspect to one side, because that is not in my remit. It is for others to decide where this role goes in future, but that is not currently part of my remit.

The key issue is that mud sticks. If you allow unregulated experimentation with technologies and the consequence of that is simply bad publicity, it really does not help the police service and others when they come to do what they need to do. That is unfortunate. For example, what possessed the Metropolitan Police to think that it would be a good idea to test facial recognition software at the Notting Hill carnival, of all places? I do not know.

Jamie Greene: That was years ago, and that was a very specific trial that went wrong. We get that. However, I do not understand the link between a seven-year-old decision that cost tens of millions of pounds for technology that is

currently sitting there and not being used to its benefit, and the modern-day environment, when we are halfway through 2022. I think that the conversation has moved on. Technology—the software and the hardware—has certainly moved on. However, are you saying that the public mood has not moved on so, as a result of that, we should not do things, because the public are against them?

Dr Plastow: No, that is not what I am saying at all. I am saying that mud sticks. The problem is that just one bad apple in the bunch changes the perception of many people.

To return to my opening point and to stick to Scotland, live facial recognition has never been used in Scotland. As I said, in the past year in Scotland, there have been no controversies whatsoever about the way that biometrics have been used for policing and criminal justice purposes.

I understand why the former Justice Sub-Committee on Policing got into that whole debate. In a sense, it was forced on it by comments that were made by Alastair MacGregor, who was the first biometrics commissioner for England and Wales and whose 2015 annual report exposed the issue around PND facial search. Of course, with the benefit of hindsight, the digital forensics issue, including the cyberkiosk experiment, probably was not handled as well as it could have been. I think that those two things came together in the minds of those on the previous Justice Sub-Committee on Policing, and drones and body-worn CCTV got wrapped up in the same argument.

Those are all legitimate policing tools, and it is not the job of any of us to tie the hands of the police behind their backs. All that we are saying is that, if they are going to use a technology—particularly a biometric one—they should ensure that they have a lawful basis for doing so and that it is used proportionately and when necessary. In other words, they need to strike the right balance between having what they need to do their job, which is to keep us all safe, and doing so in a way that does not ride roughshod over people's collective or individual human rights.

11:15

For the avoidance of doubt, I am not opposed to the police using facial recognition technology in the right circumstances, provided that it works, there is a lawful basis for it, and things are done in a proportionate way when they are necessary. To be honest, I do not think that I could be any clearer than that.

The Convener: I will bring the session to a close in about 15 minutes, and we still have a few things to get through, so please make questions and responses a wee bit succinct.

Russell Findlay: I will be brief. My question has two parts and is very specific. Jamie Greene touched on local authorities that have the capacity to use facial recognition technology but are not yet using it, and he talked about the fact that the technology is changing rapidly—day by day and week by week. Do you know of any private organisations that might be using facial recognition technology and, if so, what ramifications could that have? Furthermore, it is likely that a retailer that uses the technology will instinctively share the information that it gets with the police, and that the information would be used for policing purposes. Would you have a role at that point, or is there a worry that that would come in through the back door—through the private sector?

Dr Plastow: The short answer to your question is that that is not part of my remit under the legislation. The Parliament decided to restrict the role so that it specifically covers Police Scotland, the SPA and the PIRC.

On your question about whether private companies in Scotland use facial recognition, the answer is yes. Everyone who has an iPhone or Samsung Galaxy and has enabled facial recognition has that data collected. There was a recent case in which Clearview downloaded people's images from the internet, so, yes, this stuff is—

Russell Findlay: Of course phones contain the technology, but I am talking more about what happens on the ground in society. If the police utilise information from private companies, would you have a role in that, or do you know what the ramifications of that might be?

Dr Plastow: I would have a role if the police used biometric data that is sourced from elsewhere and that comes within my remit. My jurisdiction covers acquisition, retention, use and destruction. There are many examples where biometric data comes into the hands of the police but was not primarily collected by them. The use of that data would come under my jurisdiction and that of the code of practice.

Pauline McNeill: My substantive question was going to be about how you intend to set up the framework to allow members of the public to make a complaint if they think that their data has been misused. However, from what you have said, I now wonder how a member of the public would even know how to go about that or that their data had been abused. Maybe you could speak about that.

Your evidence suggests to me that there is a massive gap in your role. Do you think that it should be expanded? I am sorry that I did not

catch all of Jamie Greene's contribution, but I am familiar with what happened with Glasgow's CCTV cameras, and where the equipment was bought from is relevant, because that is controversial. Every weekend in Glasgow, there are protests and marches, some of which are controversial. Members of the public are probably concerned about being on CCTV, and want to ensure that the footage is used properly and is not abused. The police use CCTV, as do many other organisations, but there is a divide between the police using it and local authorities and private companies using it. That seems to be a very messy area.

You have produced a code on the substantive issues for which you are responsible, but should not your office, or another office, have some overarching view on the use and collection of surveillance data in which anyone's face appears, whether it is detailed or not? That is what has surprised me about today's evidence session.

Dr Plastow: The short answer to your question is yes. That is why, a number of years ago in England and Wales, the office of the Surveillance Camera Commissioner was created. My opposite number in England and Wales has biometrics and surveillance camera functions, and he produces a code of practice in relation to his surveillance camera function.

The first organisation to be accredited under that code of practice was from Scotland. I forget which organisation it was—it might have been Glasgow City Council, but I am not sure, although I could find out from Fraser Sampson. However, the fact that Scottish organisations feel the need to voluntarily adhere to a code of practice that is produced in England and Wales probably answers your question. There is a gap.

Fulton MacGregor (Coatbridge and Chryston) (SNP): The difficulty of coming in at the end of the evidence session is that most of the points that I was going to ask about have been covered. However, I will try to put a slightly different slant on the matter.

With Rona Mackay and, of course, the clerks, I was involved in the progress of the Scottish Biometrics Commissioner Bill through the Parliament at stages 1 and 2—obviously, the whole Parliament was involved latterly. It is good to see the fruition of that and how passionate you are about your work because, in many respects, you and your small team are the bill. The work that you are doing is really good.

I will not lie to you: if I remember correctly, the bill was very technical and involved some long mornings in committee—I am sure that Rona Mackay would back me up on that, given that she asked for my assistance earlier. It is therefore good to see somebody who is passionate about the role and brings the process to life for us as we hear about your work.

My question is about the collaborative work that you are doing with counterparts in the UK. As you said in your opening statement, there is a lot of overlap between the various pieces of legislation. You have covered most of that, but I ask you to put on record where you think the collaboration work will go in future. What are your thoughts on working with Fraser Sampson and others in future and where that collaboration will go if different legislation is put in place? For example, if other powers are devolved to Scotland, how might that work?

Dr Plastow: That is an interesting area.

The 2020 act requires me to have a professional advisory group but leaves the decision as to who should be on it to the commissioner, subject to the approval of the parliamentary corporation. I decided at the outset that I wanted Fraser Sampson along with representatives from the Information Commissioner's Office, the Children and Young People's Commissioner Scotland and the Scottish Human Rights Commission and others on that group.

The group meets quarterly. As you rightly point out, there are a number of overlapping areas of responsibility. The group allows us to discuss pertinent issues that concern us all, and the arrangement seems to work really well. As I mentioned, I managed to get myself invited on to the FINDS strategy board, which is the UK group that oversees the running of the DNA and fingerprint databases, and that works really well.

I am fortunate in that Fraser Sampson is Scottish and lives in Scotland, so he and I can meet regularly. I have met the new UK Information Commissioner but, as members will know, there is an office in Edinburgh.

The arrangements work well. However, there are areas that could become problematic. I mentioned the DCMS consultation. If, for example, the UK Government decides to hand oversight of police and criminal justice biometrics in its entirety to the Information Commissioner's Office, that would have consequences for Scotland, because it would leave a gap. Who would do national security determinations in Scotland if Fraser Sampson's post did not exist?

Potentially, that could usurp the will of the Scottish Parliament. Way back in the early days of the bill, before the creation of a new public body was even contemplated, consideration was given to whether there was an existing body out there that could take on the role. The Information Commissioner's Office was considered, but it ruled itself out.

There is a vulnerability there. If Westminster decides to go in one direction on the issue, there would be consequences for Scotland. That is an inevitable consequence of having different legislative frameworks that culminate in data all going into the same databases. It brings a whole host of problems.

Fulton MacGregor: Thank you for airing your concerns in that regard.

The other area that I was going to ask about has been quite widely covered by other members. It concerns the expansion of your role. I remember that, during the passage of the bill, there was a lot of discussion about local authorities and the various biometric data that other bodies have. Even just to get into the Parliament building, all of us who work here have to press our fingerprint down. There is a lot of that.

Rather than looking at expanding your role—I think that the Parliament has been quite clear on that—do you have any thoughts on whether your current role would be useful either for other parts of the criminal justice sector or even, in time, for local authorities or other public bodies?

Dr Plastow: Yes. Without giving away anything or everything that is in my draft annual report, another obvious area is prisons. There are 7,000 prisoners in Scotland, and they all have their biometric data captured. That data is then shared as part of criminal justice administration. I meet regularly with the chief inspector of prisons, Wendy Sinclair-Gieben, and with others in the criminal justice landscape in Scotland. If I was a member of this committee, I would be asking: who oversees that data?

Does that answer your question? That is just one example.

Fulton MacGregor: That is great—thank you.

The Convener: We have five minutes or so left. I will bring in Rona Mackay and Collette Stevenson, and then we will come to a close.

Rona Mackay: I apologise if you have covered this and I have missed it, Dr Plastow, but I want to ask about your role. Do you rely on reports coming in to you about people who have or have not broken the code of practice, or do you proactively investigate things?

Dr Plastow: The short answer is that none of that is in place yet. Until the code of practice is introduced by regulations—

Rona Mackay: But how do you envisage that that will take place?

Dr Plastow: Two essential conditions have to be met in order for someone to be able to complain. First, they have to be a data subject—for example, their data must be held by Police Scotland, the SPA or the PIRC. Secondly, that body has to hold the person's data in a way that leads them to believe that it is breaching the code of practice.

I will put my head on the chopping block here: I do not think that the process will result in a high number of complaints. The most likely complaint scenario would probably be a data protection matter, which would go to the ICO, or people might wrap up a complaint into a wider complaint about unlawful arrest or something like that. My gut instinct—it is only that—is that the numbers of complaints that we will receive will be relatively small. However, the Parliament felt that it was important that there was a means of public redress in the regulatory landscape.

That is just my best guess.

Rona Mackay: You have kind of answered my next question. If you are dealing only with police and criminal justice matters, they will know the rules, so it might be a bit quiet—the chances of your being swamped with stuff may not be that high. However, in a case where something has happened and it is found that the code has been broken, what is the penalty? Is there a penalty?

11:30

Dr Plastow: There is not a financial penalty or anything like that. The legislation allows for a compliance notice to be served on the organisation concerned. If the organisation disregards the compliance notice, the 2020 act allows for the matter to be taken to the Court of Session. I suggest that that scenario is highly unlikely, but it is important that the legislation provides for it.

Do I think that Police Scotland, the SPA or the PIRC would knowingly breach a code of practice? No. Are there areas of vulnerability for them? Yes, there are areas of vulnerability. Sorry, that is hard to say—I will put my teeth in.

There are difficult questions for them around anything to do with the face. Unlike fingerprints and DNA, which are held in single databases, facial images are everywhere. They can be on a primary, secondary or tertiary database, and there are so many of them that I do not think that anybody actually knows where they all are.

Another area of vulnerability is digital forensics, and specifically where the police or others recover biometric data—face or voice data—from people's electronic devices in circumstances in which that can enter the evidential chain from crime scene to court. There are vulnerabilities that need to be addressed now. Police Scotland has already embarked on a journey of accrediting its digital

forensics processes and procedures, but it will not complete that process until 2024.

Those are the two areas where I suggest that Police Scotland and others would need to pay most attention to ensure compliance with the code.

Collette Stevenson: You have just touched on the issue that I want to raise. To put it in context, I have a Ring doorbell, which captures people passing by the door and whatnot. I have spoken to the police about that, as there was an incident in which people were loitering about outside at 2 or 3 in the morning, and the police said that they use the system a lot. Are you saying that that could be open to a complaint, because it involves facial digital technology? Could a complaint come back to me under data protection or GDPR legislation? In addition, the company, Ring, also holds that information. I suppose that I am going down a bit of a rabbit hole here, but where does it end?

Dr Plastow: Yes—how long is a piece of string? I made the point earlier that the code covers any biometric data that is, under the Scottish definition, acquired, retained, used or destroyed. If the police obtain an image from a crime scene and retain that image for evidential purposes against the profile of an individual, that falls within the Scottish definition of biometric data, although not within the definition in England and Wales. I agree that it is a challenging task.

The Convener: Thank you, Dr Plastow. I bring the session to a close. That was a fascinating and important discussion, with a lot for us to think about, and we will certainly write to you with any follow-up questions that members have. We look forward to the publication of your annual report this summer.

11:34

Meeting continued in private until 13:03.

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

All documents are available on
the Scottish Parliament website at:

www.parliament.scot

Information on non-endorsed print suppliers
is available here:

www.parliament.scot/documents

For information on the Scottish Parliament contact
Public Information on:

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

The Scottish Parliament
Pàrlamaid na h-Alba