



Science and Technology Committee

Oral evidence: [Current and future uses of biometric data and technologies](#), HC 734

Wednesday 10 December 2014

Ordered by the House of Commons to be published on 10 December 2014.

Written evidence from witnesses:

- [Information Commissioner's Office](#)
- [Biometrics Commissioner](#)
- [Association of Chief Police Officers](#)
- [Home Office](#)

[Watch the meeting](#)

Members present: Mr Andrew Miller (Chair); Mr David Heath; Stephen Metcalfe; Stephen Mosley; Pamela Nash; Sarah Newton; Graham Stringer; David Tredinnick

Questions 82-185

Witnesses: **Dr Simon Rice**, Group Manager (Technology), Information Commissioner's Office, **Alastair R MacGregor QC**, Biometrics Commissioner, Office of the Biometrics Commissioner, and **Chief Constable Chris Sims**, National Policing Lead for Forensic Science, Association of Chief Police Officers, gave evidence.

Q82 Chair: Gentlemen, welcome to the hearing this morning. It would be helpful for the record if you would be kind enough to introduce yourselves.

Chief Constable Sims: I am Chris Sims, Chief Constable of West Midlands and lead for ACPO on forensic science.

Alastair MacGregor: I am Alastair MacGregor, the Biometrics Commissioner.

Dr Rice: My name is Simon Rice. I am the group manager of technology at the Information Commissioner's Office.

Q83 Chair: Chief Constable, if I can start with you—in your case, welcome back—the Biometrics Commissioner told us that the police were investigating applying facial

recognition software to photographs taken in custody. Can you confirm whether a searchable database of custody photographs is now being used by the police?

Chief Constable Sims: The PND computer has some access to database across the country. Most of the database, if you use that term—it is very different from using database in terms of DNA or fingerprints—sits within the custody systems of individual forces. PND potentially offers the bridge to look at it nationally.

Q84 Chair: So that would be an ambition.

Chief Constable Sims: Subject to the debate that I think you are alluding to, and to the maturing of the technology. We have had a long period where facial imagery has been talked about but has not necessarily quite lived up to its technical proficiency.

Q85 Chair: I presume the system would be such that any force could access this.

Chief Constable Sims: That is what PND does; potentially, it would bridge across.

Q86 Chair: By an individual officer.

Chief Constable Sims: I think you are now talking about the business process, if you like. We are some way off designing how the business process would work, but it is feasible to do it.

Q87 Chair: It is feasible to do it, but you have not yet decided what the process ought to be in accordance with the regulators.

Chief Constable Sims: No.

Q88 Chair: Does the database—we know it could—include custody photographs of people who were subsequently not charged?

Chief Constable Sims: It does. My colleague the Chief Constable of Durham leads on this subject and will have a more authoritative set of answers than I have, but it does. They are held in line with MoPI rather than any other legislative basis. The Committee will be aware that that is the subject of a lot of discussion at the moment, and it has been the subject of some court cases. A considerable amount of work is going on to understand how those images are held and what the future arrangements should look like.

Q89 Chair: This does come up from time to time in constituency casework. I have a similar issue bubbling in my own patch at the moment where people have their details on police

information systems, not because they have committed a crime but because they have either been a suspect at one stage, having been in the wrong place at the wrong time, or, in one case, reported a crime. Do you not think that people like that should have the right to have their data taken off systems?

Chief Constable Sims: Reporting a crime is a completely different set of circumstances. When we are talking about imagery in the way you are describing, we are talking about custody imagery. These are people who have been subject to arrest and have been photographed as part of that process. We have just been through a very long process with a similar set of considerations around DNA and fingerprints. We have a legal set of rules that are now being implemented about how long we can retain fingerprints and DNA in those circumstances. The issue is that the legislation did not directly address photographs, and that is the debate going on at the moment. There are clearly common areas, but equally there are some differences in terms of photographs as well, and the debate going on at the moment is about how those rules should be applied.

Q90 Stephen Metcalfe: I want to explore a little more what controls there are over the way you use facial recognition software. What regulations apply to its use? Is it regulated?

Chief Constable Sims: I am not aware of forces using facial image software at the moment. There are certainly lots of discussions and there has been some piloting, but from my perspective the technology is not yet at the maturity where it could be deployed, so issues as to how it is used sit as a future debate rather than a current one.

Q91 Stephen Metcalfe: From the perspective of the various commissioners, would you imagine that facial recognition software is regulated?

Alastair MacGregor: I have to say that I am slightly surprised by some of what Chris has said. It may be that I have misunderstood the position or that, as Chris made clear, this is actually Chief Constable Barton's area. It is certainly my understanding that 12 million-plus custody photographs have been uploaded to the PND and that facial recognition software is being applied to them. It is quite clear that that is happening on a local basis; it is clearly happening in Leicestershire, who have produced a number of stories about how useful it has been to them. It is my clear understanding that it is also the position with the Met, who have a database of their own to which they upload custody photographs and apply facial recognition software. It is my perception that this is more than an aspiration; it is now a reality. My concern is that it has become a reality perhaps without the issues being properly discussed.

Q92 Stephen Metcalfe: Do you want to respond to that?

Chief Constable Sims: I am equally surprised. I certainly did not think it was an operational reality. I thought these were pieces of development work under discussion, but I absolutely bow to Alastair's knowledge on the subject.

Alastair MacGregor: Never do that.

Chief Constable Sims: This is not my area of specialty.

Q93 Stephen Metcalfe: Let us assume for a moment that it is happening. What regulatory framework is in place to control that activity?

Alastair MacGregor: As far as application of the software is concerned, I am not aware of any regulatory framework that is applied. The question of the value and validity of the algorithms and so on is presumably a matter considered by forces individually and/or by the Home Office's Centre for Applied Science and Technology. It is my understanding that at the moment CAST is looking at the algorithm applied to images on the police national database. I am not aware of any external regulation of the quality, but it is a matter that I know is of importance to the individual forces concerned. One of the points raised with me was that there were doubts about the reliability of the software used on the PND, and that was one of the reasons why it was being looked at. The software in this whole area has developed. It was not terribly reliable, but it has improved fairly dramatically in the last few years.

In fairness, you will appreciate that, as I made clear in my own submission, this is not my area either. My responsibilities cover simply DNA and fingerprints, as does the Protection of Freedoms Act. My interest in this is therefore not as someone who is active in the field, but as someone who sees that similar issues arise.

Q94 Stephen Metcalfe: Who is regulating? Who is in charge, or is it just the wild west out there?

Alastair MacGregor: That I do not know. In terms of the quality of evidence that goes before a court and so on, general facial mapping evidence is a matter for the forensic science regulator and so on. As to who monitors or assesses the value of the software that is being used, it seems to me that that has to be a matter for the forces, and possibly for the Home Office.

Q95 Chair: Is it not a bit odd that your role is just that narrowly defined bit? We heard powerful evidence in an earlier session from Sir John Adye. He said that biometric evidence, to be worth a lot, has to be cross-referenced to several data sources, and that you do not rely on one biometric. It seems a bit odd that the Office of the Biometrics Commissioner does not cover all potential biometrics.

Alastair MacGregor: That is what Parliament chose in the Protection of Freedoms Act. They addressed the issue—

Q96 Chair: Parliament does occasionally get things wrong. We have all seen mistakes. Are you saying, Mr MacGregor, that Parliament ought to revisit that because it is not logical?

Alastair MacGregor: I am keen not to empire-build. I assure you that I have quite enough to do at the moment. There seem to me to be obvious parallels in the issues that arise in relation to at least those three biometrics, and there would be some value in external oversight of them because, among other things, this is an important area. Clearly, these technologies can be of enormous value in the prevention and detection of crime, but equally clearly they will be undermined unless the public have confidence in them and feel that they are being properly run and supervised.

Q97 Mr Heath: It is not just whether public confidence in the technology will be adversely affected but whether it will be admissible and have evidential value. If it has no probative value because the various regulatory mechanisms do not mesh together, it makes the use of it by police forces completely pointless; they cannot use it in court.

Alastair MacGregor: Yes and no. It is being used at the moment for investigatory purposes only. No one is being prosecuted simply on the basis of, "We've got an automatic match," but in terms of investigations it is still very important. If you get a match, or appear to get a match, that can send the investigation off on the wrong route altogether and create difficulties. Alternatively, it may lead to or play a part in the decision to pick up that person and start questioning him, which may be less amusing for the person involved.

As I mentioned in my submission, it seems likely that a fair number of images are being unlawfully held; in reality they should not be held, and therefore they should not be processed. To pick up your point, there might be a challenge at a future stage: "You were using material that should not have been there at all."

Mr Heath: Or that should be there.

Q98 Stephen Metcalfe: I think we have stumbled into privacy issues. There is no regulation. We have no idea whether or not the software is reliable. Different forces may be using different algorithms. Some forces are unaware that other forces are trawling through databases and pictures and applying them for the detection or prevention of crime. No one seems to be regulating it. You are not convinced that you want to take on this role. Surely, we cannot just leave to chance that the benefits outweigh the downside of it.

Alastair MacGregor: Absolutely. That is why I raised it with the Committee. There has been very detailed and considerable public debate about what should happen about DNA and fingerprints, whose material should go on the national databases and how it should be supervised and so on, yet this separate but entirely comparable mechanism has developed without that general debate. My concern is not to suggest what the answers are, but it is right that those issues should be addressed. You are right: clearly, privacy is of central importance.

Q99 Stephen Metcalfe: The Information Commissioner might want to come in at this point. Dr Rice, I believe your office recommended that a privacy impact assessment be made by the police forces using this. Are you aware of whether that has or has not taken place?

Dr Rice: First, I would not say that this area is completely unregulated. It is outside the biometrics commissioner's remit, but if an individual is identifiable from the photographs, or if it is part of their national record, it would be personal data and therefore regulated by the Data Protection Act. We would obviously look for a lawful basis for its collection and retention and for any particular process, whether facial recognition or not. We recommended a privacy impact assessment which would assess particularly those issues. I am not aware of any that have been done. It is not a legal requirement for a police force to submit that to us for prior authorisation.

Q100 Stephen Metcalfe: We talk about false positives and false negatives when we look at other areas of science. What I am trying to get at is that, without regulation or anyone collecting data on this, we do not know, or I assume we do not know, whether or not this is working and whether it is a fair use of technology, or whether lots of people who have no connection are being investigated because their faces happen to look like someone else's.

Alastair MacGregor: Yes, but it is unfair to say that no work is being done. I am aware that CAST is looking carefully at the central algorithm and trying to assess its reliability. I know, for example, that the Met have great concerns about the quality of software, and that is something they look at all the time. I do not think people are indifferent to it. As far as police forces are concerned, it is of no value to them unless it is reasonably reliable.

Q101 Stephen Metcalfe: Do you want to add anything to that?

Chief Constable Sims: No.

Q102 Stephen Mosley: Given what has just been discussed, do you think there is a need for a national strategy for biometrics?

Alastair MacGregor: Clearly there is value in a national strategy in that field. At this very moment a meeting is going on of the forensics and biometric policy group, which is concerned with the development of a national strategy for both forensic science generally and biometrics. That is quite a large and wide-ranging group, so it is perhaps unsurprising that it has not been that easy to develop one. It is a committee that Chris is on, and I attend as an observer. Looking just at biometrics, clearly there is value in someone looking forward and trying to identify what challenges are to come, what sort of governance arrangements are going to be needed and all the rest of it. One can only welcome that, so it is desirable.

Q103 Stephen Mosley: I put this to all of you: what contact have you had with the Home Office in terms of pushing this forward?

Alastair MacGregor: In terms of this image database/facial recognition issue, with respect, I think I made that clear in my written submission. I attended the meeting in April when I discovered this and understood that it was happening. In fairness, a representative of the Home Office was present at that meeting and also had concerns to discover that it had gone into operation so quickly. I wrote to the chief constable concerned and I also raised it internally with the Home Office, and I know it was raised by others. I then had a series of meetings with officials in the Home Office raising the issue and suggesting that it really ought to be addressed. Again, in fairness, they generally recognised that there were issues that had to be addressed, and, as I understand it, attempts have been made to take the matter forward. Quite how successful those attempts have been I am not sure.

Q104 Stephen Mosley: Has the Information Commissioner's office been in contact?

Dr Rice: We have certainly been in contact again with the Biometrics Commissioner in many of those meetings as well, but we also followed up reports with individual police forces to see how their biometric systems might be being used for their purposes, and that sort of thing.

Chief Constable Sims: Mike Barton, Chief Constable of Durham, is leading that work with the Home Office. I guess that it is an attempt to get some equivalence of governance and data management in a new and different emerging area.

I would slightly take issue with Alastair. I do not think there is exact equivalence between DNA, fingerprints and imagery, but there is enough to think that we would want to walk down a similar path to get to a similar position. I think a strategy would help to crystallise that and move it forward.

Alastair MacGregor: On the specific issues, it is my clear understanding that it is now recognised—and, what's more, was quickly recognised—by the Home Office and other stakeholders, such as the police and so on, that there are important issues that ought to be addressed. In particular, among other things, something had to be done about cleansing the database of material—photographs which should not be there, even on the basis of the existing law—and a new retention regime should be developed, and proper governance brought into existence in this whole area, which I think has been touched on by you on other occasions.

These are not easy problems. The technical difficulties of cleansing the database of questionable images, or images that should not be there, are, I understand, very considerable. Difficult legal and technical issues arise as to what the appropriate retention regime should be. You could just read across from DNA and fingerprints. That would perhaps be a sensible and easy way through, but, as Chris says, there is an argument that facial images are rather different and there should be a different regime.

Q105 Stephen Mosley: Going back to the discussion we had about the police national database, do you know who made the decision to upload photos to the national database? Was a specific decision made?

Chief Constable Sims: I think it was always the intention. It was not a decision. The database sits across 43 force intelligence systems and custody systems, so it was designed specifically to do just that.

Q106 Stephen Mosley: The design of the software up front included the ability to upload photographs and biometric data.

Chief Constable Sims: Yes. Let us remind ourselves that PND was brought in on the back of Soham and the Bichard report, and it was there to make visible across the country the intelligence held by individual forces. From the start, custody information was scoped into that; it was always the intention of the PND project that it would look across and be able to see custody images.

Q107 Pamela Nash: I'd like to turn to public attitudes to biometrics, which we touched on earlier. Can I ask each of you generally what your perception is of current public awareness and attitudes to biometrics and the use of them?

Alastair MacGregor: I cannot pretend to any great expertise in what the public think. It seems to me that the attitudes range from the extremes of "Done nothing wrong, nothing to worry about" and/or "Privacy died long ago and no one under 30 gives a damn, so why are you concerned?" to those on the other side who have increasing concerns about what they see as the surveillance state, particularly when you have much more widespread high definition CCTV and so on—body-worn video and that sort of stuff—who take the position, "I'm a citizen, not a suspect."

As to where the centre of gravity lies, it seems to me that it slightly depends on what the last story was in the press, or the last Hollywood blockbuster. People are concerned, and they recognise that there is a difference between the commercial use of biometrics and the state's use of them. They realise that commercial uses are very concerning. People worry that Mastercard and Tesco know a great deal more about them than they would like them to know—about their spending habits, movements and so on—but they are also conscious that, at least in theory, they have a choice; they can stop using their Mastercard or Tesco Clubcard, and they chose to use them in the first place. It is rather different when they are concerned with the state's use.

Q108 Chair: With respect, the one about store cards is a little naive. It is all right for you and me, reasonably well-off people, to say that, but poorer people cannot make that choice. The discounts are there and they have to use these things.

Alastair MacGregor: I accept that. I did say there was a certain notional. The other point is, "What harm does it do me?" I am bombarded with all kinds of adverts that I do not want and it is tiresome, annoying and so on, but the situation in relation to Government or police use of biometrics is rather more worrying to me. It is not just the distinction in consent—that I can stop doing it. It is also the fact that, first, I am obliged to give them if I have been arrested and that, secondly, what can be done with them by the

police might be a great deal more troubling for me than what can be done by Tesco—I do not want to direct it particularly at Tesco—Sainsbury’s or John Lewis, annoying though it is, particularly today.

Dr Rice: A lot of it depends on the context. We have already discussed private sector usage versus law enforcement usage, but even within those there will be separate distinctions, whether it be for intelligence purposes, surveillance purposes and things like that. In terms of specific queries to our office, I did a search on our system yesterday. We have had only five inquiries specifically referencing biometrics.

Q109 Pamela Nash: Do you mean five people with queries about their own biometrics being misused and mishandled?

Dr Rice: About biometrics being used in some system.

Q110 Pamela Nash: Would it be about personal data, or just someone with a general concern?

Dr Rice: It would be about personal data. One of them was about a high street bank: “Is it lawful for them to collect my biometrics for some kind of processing?” There are three from parents about a fingerprint-based system being used in a school. They are just asking, “Can they do it? Is it okay for them to roll out the systems?”

In contrast, the IP camera blog was talked about in the previous session. To put that in perspective, that has now been read 43,000 times. Compared with that number of cases, it highlights that when you present the problem to the public they appreciate it and may take the necessary action rather than thinking perhaps, “Should I be concerned in that instance?” Certainly our role in that education is to help people make the right choices.

Chief Constable Sims: Like my colleagues, I cannot quantify what the public view is. I have held a role as a senior officer around DNA and fingerprints for 16 years. I have done countless public debates on the balance between liberty and security, and I can absolutely vouch for the fact that there is a massive range of different views and, as Alastair said, it is very hard to quantify where the balancing point is in the middle. Making that judgment is probably more Parliament’s role than mine.

ACPO absolutely recognises that if we are going to take forward the use of these technologies to protect the public, we have to work hard to maintain their legitimacy. If you take DNA as an example, there is a DNA board that oversees the database and its use. An ethics group sits as part of that board and provides advice, and there is a national reporting process in terms of how that data is used—a really strong system of governance. ACPO has been desperately trying for several years to get a similar level of transparency in governance established around fingerprints, but it has been really hard work. At times we have felt we are the only party interested in doing that. Some of my colleagues might vouch for that, as they have been part of that process. We have not managed to get a lot of traction for that to happen. I am pretty certain that my successor will be sitting in front of this group in two or three years’ time talking about a similar debate around imagery. There

is a natural roll-on, but if we do not get the understanding and support of the public, which I strongly believe is based largely on transparency in the way we operate, it is absolutely clear that we will not be able on their behalf to push forward to use these technologies in the way that best protects them.

Q111 Pamela Nash: Do you think the Government have been less willing to engage in this debate in informing the public because of the furore about identity cards and biometric identity cards?

Chief Constable Sims: The legislation before last—the legislation drafted in the last days of the Labour Government—was accompanied by a decent attempt to engage with the public to try to present a statistical view, if you like, of why the data is held. I think there was a reasonable debate then. That did not quite happen with the last legislation, because in a sense that debate had already taken place—perhaps there was already an agreed point for the legislation to move forward. There have been attempts to do that. Sometimes I am not sure that the wider public is as interested in that debate as perhaps a narrower group engaged in it day in, day out.

Q112 Pamela Nash: Absolutely. I am sure I am not the only one at this table who has had lots of e-mails from lobby groups about this, but I think that in four years I have only had one constituent raise it on the doorstep. Dr Rice, I referred to Government, but do you think that in general politicians have stepped away from the debate about this because a bad taste has been left in their mouths as a result of the coverage of the introduction and cancellation of identity cards?

Dr Rice: Certainly the public reaction to ID cards was not very positive, perhaps leading to the cancellation, but I do not think the public have shied away from biometrics or somehow been turned off. It is worth recognising that there is a difference between using your fingerprint to access the gym and giving your fingerprint to a Government institution, or even to the police, with the image of standing in the police station rolling your fingers over the ink pad to give your fingerprints. There is a great distinction between the two, and they will certainly be used for very different purposes, and that distinction will be in the minds of the public.

Q113 Pamela Nash: That is why it was interesting that you referred to the schools issue, because it is not compulsory for young people to give their fingerprints.

Alastair MacGregor: The use in schools is often an inquiry that I get. That is regulated to some extent under the Protection of Freedoms Act. It is necessary to get express permission from parents, and children must be able to opt out. People do get concerned about it. So much seems to depend upon what the last story was. I am conscious that one press story will be, “DNA of rapist lost. Scandal,” and the next one will be, “DNA from eight-year-old children held. Scandal.” It is very difficult to know where the centre of gravity is, but you are right; a large number of people are not very concerned about it, at least in terms of commercial use. I think more people are concerned about Government

use. In fairness to Chris, it is quite clear to me that the police recognise all these issues and are very keen to make sure there is proper public buy-in to them. They have done a great deal. The way in which DNA is governed and regulated seems to work very well. I know efforts are being made to try to make the same true of fingerprints, and it seems to me the same should be true of other biometric technologies.

Q114 Sarah Newton: To pick up on public confidence, one aspect we have not discussed is the storage of data, because I think everybody would be concerned about identity theft and how their biometric data could fall into inappropriate hands. Unlike a PIN, you will not be able to get back your biometric data if somebody has stolen it and then uses it. You could be left in a situation where you could not even verify your identity. In your evidence, Dr Rice, I think you said that biometric data must be transformed and stored in a non-reversible form. What steps do you take to ensure that that standard is adhered to?

Dr Rice: The standard in the Data Protection Act is that appropriate security measures must be taken. There are certainly similarities between this and the storage of a password, for example. A password should not be stored in plain text so that if there is a breach, an attacker can use that password and gain access. As you have highlighted, you can revoke and change a password, but it is not quite so straightforward—it is almost impossible—to change your fingerprint.

There were some discussions with the previous panel about transforming that image into a template to bring out the important features within a fingerprint and store them in some kind of format, so that you cannot go back to the fingerprint and take the template to create some kind of spoof latex fingerprint to gain access. Those would be the sorts of things we would be looking for. The ideal is that if that biometric data is breached in some way, it should not matter to the individual. You should be able to re-enrol a person with a new biometric, and that template should not be able to be used in some other kind of system to gain access.

Q115 Sarah Newton: You describe the scenario very well, but I have not really heard what steps you actually take to make sure these ideas are adhered to by people who are storing it. It could be schools, sports clubs or the police. What steps do you actually take to ensure those protections are in place, and to what standards are you operating?

Dr Rice: It would be up to the institutions rolling out the biometric system to make sure they are storing it in that way. We have guidance on our website about fingerprints, although it has now been replaced with guidance from the Department for Education in that regard, but it is something we would look at in any investigation.

Q116 Sarah Newton: It is something you look at in an investigation, so you do not ask up-front for solid information which you can absolutely check to a template and a standard, but if something goes wrong you investigate to see whether they did or did not, or maybe I have misunderstood what you said.

Dr Rice: It is not there in the legislation that the data controller must write to us for approval before they roll out a particular system. If they got in contact we would help them choose from what is available on the market, and in the case of the Government, or some other body, procuring a system, they can use their power to make sure they get the right system to store the data.

Alastair MacGregor: There is a difference between commercial organisations and what actually happens in Government in the context of DNA and fingerprint databases. There is huge attention to the security of that information. I think that under 40 people have access to the DNA database. There are all kinds of supervision by UKAS and others. I am not aware of any occasion on which it has been suggested that information, or biometric information, has leaked from the fingerprint or DNA databases, or even local police databases of fingerprints.

Chief Constable Sims: It has been strengthened by the recent legislation; particularly in the case of DNA, we no longer store samples. All that is stored are numerical profiles detached from nominal data to protect against what you describe. Both for fingerprints and DNA, these are systems operated nationally under very tight guidelines, so a great deal of security is built in.

Q117 Sarah Newton: Can I ask a question of Alastair, the forensic science regulator?

Alastair MacGregor: If I may interrupt, I am the Biometrics Commissioner, rather than the forensic science regulator. His area of control is very much wider.

Q118 Sarah Newton: I stand corrected. That regulator has published a code of practice and conduct which references BSI standards, so why is there not an equivalent code for biometrics?

Alastair MacGregor: With respect, this is not my field. The forensic science regulator does things in terms of standards and so on—for example, in relation to what has to be done when you are deriving a DNA profile from a sample. There are already quite significant laboratory standards required, but that is not my area. My area is about police retention and use of this material. Whose material should be on the databases, and what should be done with it? I'm afraid that's one for the regulator.

Q119 Sarah Newton: In that capacity, when you are in an advisory role and part of panels, are you aware of any consideration given to the storage of biometric data and the regulation of its storage?

Alastair MacGregor: Yes. Chris mentioned the fact that we no longer retain, except in relatively small numbers, the DNA samples. About 7 million used to be retained. One of my jobs from the beginning was to try to establish that they had all been destroyed, as appeared to be the case. It seems to me fairly clear that they had.

In terms of the quality of the reassurance as to the information on the databases, and that it is not leaked, I look at that and know there is important oversight—external as well. I am not a technician in this area, but with UKAS and so on, all kinds of steps are taken to ensure that the information is safe. Nothing I have seen has led me to believe there is an absence of clear enough standards.

Q120 Sarah Newton: Does anybody want to make a final comment before we move on?

Chief Constable Sims: I agree with that.

Q121 Chair: It sounds a bit of a muddle. Chief Constable, if you recall, you appeared before us in our first inquiry into forensics. After the second inquiry the Government response was that there needed to be a joint strategy covering forensics and biometrics. That was more than a year ago. Mr MacGregor is saying that it is not his bailiwick. I don't blame him for that; his functions are limited by statute. A strategy has not been developed, and yet we are all in the same place round this table, wanting to ensure that the best interests of criminal justice are served, at the same time as maintaining the rights and privacies of ordinary citizens. There is no dispute about that. You really do need that strategy put in place pretty damn quick.

Chief Constable Sims: I agree. The landscape that has been created is quite complicated. You have Alastair's role, you have the forensic regulator and you have the databases now sitting within the Home Office. From memory, around the time you were taking evidence last time, the NPIA was being shut down and the forensic science element of the NPIA was migrating back to the Home Office. There is no doubt that that has added some complexity.

ACPO has an operational strategy that is about improving the way we work—our effectiveness; improving legitimacy and transparency in the way we deal; managing innovation, and so on. That has to sit within a much broader piece that is operated through the Home Office and Government. That is the bit that is still subject to some debate to get to the point where we have an all-embracing national strategy. I absolutely need that to happen, because a whole set of significant issues and risks sit within forensic science. One or two of those have surfaced today, but there are many others. The way those risks are mitigated and managed is through that national strategy.

Q122 Chair: In terms of things that are within your remit, Mr MacGregor, you talked about changes to the way DNA information is being stored. Presumably, you are working very closely with the police on data from samples related to unsolved cases, or cases that are still live. There must be a mechanism for protecting the integrity of that data.

Alastair MacGregor: Yes, essentially it is an investigatory matter, but we work closely together. In terms of the strategy, as I mentioned and as Chris said, it has not just been forgotten as something that needs to be developed. Efforts have been going on to develop it, but clearly it has not been easy. In the area of biometrics, one of the issues to consider is: what are the new technologies likely to be? What challenges will they throw up? For

example, we have been talking about photographs, and we have got DNA and fingerprints, but speaker recognition is likely to be the next one, or another one.

Q123 Mr Heath: I think that goes into the area that I want to discuss. We accept the evidence you have given—that there are lacunae in the current legislation in terms of organisation—but on this Committee we very often find that there is a race between technological advance and legislation. Technological advance always wins and Parliament never catches up. Mr MacGregor, you mentioned a couple of areas where you feel that biometric technology is running ahead of legislation. Are there others you could identify for us? Dr Rice, I ask you the same question.

Alastair MacGregor: Not immediately. Facial recognition was clearly the next one. Speaker recognition is also now being used quite widely commercially, and will be used more by Government. As I understand it, we do not yet have significant databases, but that would seem perfectly sensible.

Chief Constable Sims: A lot of our efforts at the moment are focused not so much on extending the range of areas we look at, but on how we make best use of the areas we have. For example, the ability to take a rapid DNA sample at scene and get an instant match is probably an area that is more operationally interesting, so that we maximise what we've got. To be frank, at a time of austerity there will not be big increases in national infrastructure. I think it is going to be about how we make use of what we've got.

Q124 Mr Heath: Dr Rice, I think you extend into non-police areas where perhaps technology is more likely to be more widely taken up and used in different ways.

Dr Rice: We have seen public attitudes to voice recording. There has been an enforcement notice against Southampton city council relating to voices being recorded in taxis. That is not suggesting that voice recognition was going on; it was purely the recording of voice. That is probably becoming a bit more sensitive in public attitudes.

On the consumer side, smartphones and tablets will record all sorts of additional data. On the consumer health and well-being side, people can record their heart rates during runs, and their locations; there are also bands that record steps. Though not strictly a biometric, it is certainly a recording of biological measurements. If you have enough of them, you can build up a picture and identify an individual from that.

Q125 Mr Heath: Our iPads are probably recording all sorts of things about you at the moment. Given that we have these changes—obviously all of you do a bit of horizon scanning in terms of where things are going—do you have a role as regulators in advising Government as to where legislation is currently inadequate, and what is likely to be on the horizon that we are likely to have to deal with?

Dr Rice: The Data Protection Act itself has stood the test of time reasonably well, because it is technology-neutral and fairly flexible. Those ideas of transparency and fairness will

cross over into all sorts of different technologies, as well as the security requirement. It is certainly our role to educate policy makers and Government, as well as members of the public, through our guidance, blogs and websites.

Q126 Mr Heath: Mr MacGregor, no formal advice would be rendered from your office, for instance.

Alastair MacGregor: I have an annual report, which I think is going to be published around the 16th of this month. Part of what I am doing is reporting on what is being done in relation to use and retentions. I hope I am also alerting Government and others to areas where difficulties have arisen, or there may perhaps be a lacuna, and where it is worth looking again at the legislation, and various issues like that. I see it as part of my job to alert them to difficulties rather than saying, “This is your answer. What you ought to do is just apply this,” and the report includes more or less the written submission I gave you. It seemed to me that it was relevant.

Q127 Mr Heath: Presumably in the case of the police it would be ACPO and/or the Met directly to the Home Office.

Chief Constable Sims: The Met is part of ACPO.

Q128 Mr Heath: I know it is.

Chief Constable Sims: We live in perfect harmony. We certainly have a relationship with the Home Office around issues where legislation is proposed. There is a huge tail of work in implementing some of the legislation on which we work very closely with the Home Office to manage.

Q129 Chair: In terms of the changing technologies that keep emerging in all parts of this discussion, what oversight do you have—I am asking the two regulators—of the testing regimes, as to whether the biometric systems produced by A N Other third party meet the kind of standards you would expect to see?

Dr Rice: The standard will depend on the context. The accuracy you would want from Heathrow airport or law enforcement would be very different from an advertising board that predicts gender, for example. There will be very different acceptable error rates. In addition, thinking about the impact on the individual would come into the mix. One thing we are embarking on is a privacy seal scheme, whereby the Information Commissioner will accredit a third party to audit and award privacy seals to a certain type of technology. We have not specifically decided which technologies; we will be opening up invitations for third parties to submit to us what they think can be regulated in this way, but biometrics would be a good possibility.

Alastair MacGregor: I am dealing only with police use and therefore the technologies being used by the police. To some extent the qualities that are there are a matter for the forensic science regulator, ACPO and the whole procurement programme.

Chief Constable Sims: There is a really good example that might illustrate the different relationships involved. In a previous answer I mentioned rapid DNA, which again is an emerging technology around the ability to sample DNA remotely and search the database. Very recently, we had a meeting of a group chaired by the regulator—the forensic regulator, who ultimately has an interest in standards. It has CAST—the part of the Home Office that does scientific development—who do type approval around new technology. It has ACPO and representatives from individual forces, who obviously are there in terms of how and in what circumstances the technology is used. There are two other parties. On many occasions, but not that one, there are academic researchers, if we require an objective external view, and nearly always there are suppliers of the technology, who also have responsibilities, and indeed an interest, to make sure that the technology is validated and approved.

Q130 Chair: You would expect the technology provider to come to you with robust data about the integrity of their system.

Chief Constable Sims: Yes.

Q131 Chair: As a smart procurer you ought to be doing that, although I shall not drift into police procurement of cars.

Chief Constable Sims: It is long before procurement.

Q132 Chair: You may call on academic research, but before putting something into the field would it be your practice, or are you required, to test your views with the regulator before things go into the field?

Chief Constable Sims: It will be slightly different in different circumstances, but there would always be a process of piloting and oversight of the objective results from the piloting. The validity that a manufacturer gives is not the same process as objectively securing actual usage.

Q133 Chair: It seems to me that it would be good practice for you to test your views off the regulator before you put things into the field.

Chief Constable Sims: Yes. In this instance, the regulator chaired the coming together of those separate areas.

Q134 Sarah Newton: I would like to go back to something Dr Rice said. I understand you want to be a proportionate regulator, and that is commendable. What is concerning me is that it seems—correct me if I am wrong—that you are applying one set of standards for how people are storing data, images or fingerprints if they are used commercially rather than if they are used in the criminal justice system. Can you not see the effect that, as more and more data are collected voluntarily with people passing it over, whether consciously or subconsciously, and being held by data storage people, there will be a honeypot effect for criminals, who will be very motivated to steal people’s data? It might be much easier to get that data, because a sports club is not asked to regulate the storage of fingerprints in the same way as the police are. This could lead to a great deal of identity theft, which will be a great concern to people.

Dr Rice: There would be not quite one standard across the board, but we would want to take that risk-based approach, and think about the risk to the individual and the quality of the data. In that regard, we would not expect a sports club to be holding fingerprint data of the same quality as law enforcement. It should not be possible. It would be of lower quality. You would not necessarily be able to use a fingerprint from a crime scene and match it against the fingerprint database of the sports club.

Q135 Sarah Newton: Is that something you absolutely check, so you know that it is not the case? From what we are hearing, it does not seem that any consistent standards are being applied to anybody who is allowed to collect somebody’s fingerprints, however benign or positive the intention seems to be. What are the standards that you use? How do you know that is not the case?

Dr Rice: We will not go into every organisation in the United Kingdom and do that test.

Sarah Newton: There we are: no standards.

Q136 Chair: Perhaps I may put a couple of brief questions to finish off. Chief Constable, you stated in your evidence that the forensic service was in a state of flux, and you reinforced that in your comments today. I think our two reports have highlighted that as well. Has that affected the way you are able rigorously to test the reliability of some of the technologies we have been talking about today, like facial recognition software?

Chief Constable Sims: No, I do not think it has affected the quality of what we do. The premium always has to be the quality of what we do, because that is the piece that enters the evidential chain and is absolutely critical. Where the state of flux has a bearing is on the future of forensic science in this country against a background of austerity, market challenge and so on. Those are probably the issues that concern me most.

Q137 Chair: You share this Committee’s view that there needs to be a serious focus on that. We are hopeful that the new regulator will exert authority over some of the remaining challenges, because if we do not do that, criminal justice will be damaged, either from the

point of view of failing to get a successful prosecution or potentially somebody being wrongly prosecuted.

Chief Constable Sims: To reiterate, in terms of the quality of the way individual cases and information are managed, which is the role of the regulator, we are absolutely committed and continue to operate to the highest standards. The issue is about sustainability of the organisation and the pressures that sit over that.

Q138 Chair: Mr MacGregor, I know that the ICO report that goes to the Home Secretary is, as a matter of statute, laid before Parliament and published. Is that the same with yours?

Alastair MacGregor: Indeed. It is for her to decide whether or not there are any bits that she wishes to excise, simply because I cover areas of national security as well. I also cover retention and use by the police for national security purposes in that context, but I am not anticipating—I may be wrong—any difficulty there. It has gone to the Home Secretary. I understand it is likely that it will be laid before Parliament on the 16th of this month.

Q139 Chair: We look forward to seeing that.

Alastair MacGregor: The film rights are still available.

Chair: Gentlemen, thank you very much for your evidence this morning.

Examination of Witnesses

Witnesses: **Lord Bates**, Parliamentary Under-Secretary of State for Criminal Information, Home Office, and **Marek Rejman-Greene**, Senior Biometrics Adviser (Deputy Director), Home Office, gave evidence.

Q140 Chair: Gentlemen, welcome to our session. Lord Bates, welcome to this end of the corridor. It is a long time since I saw you at this end; it was back in the 1992 Parliament. Welcome back. Perhaps your colleague would be kind enough to introduce himself.

Marek Rejman-Greene: I am Marek Rejman-Greene, senior biometric adviser at the Home Office, and I also work out of CAST—the Centre for Applied Science and Technology.

Q141 Chair: Do you think the public accept that the emergence and roll-out of the widespread application of biometric technologies is a foregone conclusion?

Lord Bates: I was listening to the discussion before. When you ask the public, it depends on the question you put to them. When you present a grainy CCTV image of a missing child, I do not think there is a parent, or a human being, in the country who would be unwilling to sacrifice any amount of privacy data to try to identify and protect that person

as quickly as possible. Alternatively, people rightly get very suspicious about big government and intrusiveness—people using their data for reasons of which they are either not aware or have not consented to. I think that is the reason why in all we have done we have tried to hold to a position of balance, trading off those two pressures. In my reading of it, I do not think we will ever reach a point where we can say this is where the balance will be. It will shift, driven by events and technology, but it is a balance of which we are very conscious.

Q142 Chair: In your written evidence you used the phrase “direction of travel”. I think you heard us question the previous panel on the absence of a strategy that was promised in our previous report. Where is the direction of travel, and how does that impact upon a strategy that the chief constable is clearly looking forward to having?

Lord Bates: You have been around Whitehall and Westminster long enough to see that sometimes strategies are offered as a panacea and they do not always deliver on that. The general argument is that there should be some bringing together of the various elements of Government, and of course that happens. I think the biometrics commissioner pointed out that the cross-Government forensics and biometric policy group is meeting at this very point. One of the things they are addressing today is whether there is a need for a strategy. I do not have a read-out from that yet, but I know that I have another appointment with the Committee in January, if invited, as part of the legacy review. I would be very happy to respond to that point in more detail, or in advance in writing, should you so wish.

Q143 Chair: That would be very helpful. Can we press you a little further on the cross-Government activity that is occurring? I take it by that that you mean “cross-departmental”.

Lord Bates: Yes.

Q144 Chair: I guess it takes into account the spectrum of applications that we heard about in the previous panel: from access to schools or sports clubs through to issues around the criminal justice system. Would you expect the strategy, if that is the right word, to start to define where the limits are for applications within different Government sites?

Lord Bates: Yes.

Q145 Chair: For example, there has been recent publicity about the acceptability or otherwise of fingerprints in schools.

Lord Bates: Partly, it would be a case of joining together in one easily accessible place what those limits are. Through the Protection of Freedoms Act, the Data Protection Act and the Human Rights Act we have a broad principle-based approach to this, about lawful purpose in the retention of data, and the balances—people’s right to privacy and family life, and so on. There are broad principles. We have heard about court cases, judgments and technology, which seems to be changing almost by the week. Sometimes, in a fast-

moving area, that broad principles-based approach can be more suitable, but in terms of the response it is happening on a cross-departmental basis through the forensics and biometric policy group. Ministers will obviously take the advice of that group as to what action they feel is needed in this area, and will respond.

Q146 Chair: In the final part of the Biometrics Commissioner's report he explains that some of his work is in the classified area, but a lot of this work needs to carry public confidence with it. The forensics policy group does not seem to be terribly transparent. It seems to me that it would help public confidence if a lot more of these discussions were not only transparent but that external bodies could have the right to make inputs into them.

Lord Bates: Yes, I think that is broadly what should happen. As part of public confidence, people need to recognise that, for example, when we talk about reports going up to the Home Secretary—whether it has been cleared, what can be redacted and so on—in statute there are very clear limits as to what can happen. It can only be on national security grounds, or in cases where there is an ongoing police investigation, or where there are other risks. In other words, it is not simply that it is an uncomfortable truth, or something we would not like in the public domain. It is not that type of editing; it is something which goes across all areas, whether it is the independent inspector of terrorism or borders and immigration. Sensitive work is going on by the police and security services to keep our country and borders safe, and sometimes that means some things cannot be released into the public domain, but the public should have confidence that, where that is not the case, they will see the reports.

Q147 Stephen Mosley: In a report on identity cards by our predecessor Committee in 2006, the then Government reassured the Committee that there were a couple of scientific advisory committees: one was a biometrics expert group and the other was a biometrics assurance group. They were looking at biometrics and providing scientific advice to the Government. In the 2014 list of scientific advisory committees neither of those groups appears. Do you know what happened to them, and who now provides independent scientific advice on biometrics to the Home Office?

Marek Rejman-Greene: The Biometrics Assurance Group was formed at the request of Parliament specifically to look at the national identity scheme. As that scheme was beginning to go into roll-out, the need for it began to be less pressing. In addition, the loss of one of the members of that Biometrics Assurance Group, who gave evidence last time, meant we were missing a considerable part of the industry inputs. The decision was made that that was no longer as pressing. There may well be a question about whether it should come back again, but it is up to yourselves to make those recommendations. Regarding the working group, there is a technical Working Group within Government which has access to specialists who are on that group. It is called BWG—the Biometric Working Group. Again, I think it was referred to in the first hearing.

Apart from that, we have very close relationships with CAST and all our opposite numbers in other Governments. We have continued relationships and discussions with academics and suppliers to understand where the current technology is and where the issues are. We

also take note of criticism, perhaps from people who have a concern about the use of biometrics, to make sure we have a full understanding of the context against which all of this advice should be given to Ministers in the Home Office.

Q148 Stephen Mosley: In one of our previous evidence sessions we heard from Andrew Tyrer of Innovate UK, who made the comment that a lot of the testing of biometric systems was done by the manufacturers themselves. Does the Home Office make any independent testing, or does it just rely on their assurances?

Marek Rejman-Greene: There are occasions when we do it ourselves and occasions when we monitor the way in which suppliers undertake the testing. One example is the use of biometrics for control of access to buildings for critical national infrastructure; if you have a data storage room, you want to make sure you can use biometrics to identify individuals who can go into that data control room, or not. A standard was developed in the UK, which we are hoping to move towards a European standard. That testing is contracted out to the National Physical Laboratory, one of the key leaders in this field.

Another example is IABS, which is a system used for immigration and asylum seekers—the 18 million people who applied for visas and asylum. That system was tested prior to delivery, and met the requirements placed on it by the user community, so we do that. It is expensive and time-consuming, so there is a need to balance the depth of the testing against the benefits and uncertainties.

Q149 Stephen Mosley: We also heard from Professor Amoore, who said that in the rush to adopt biometric technologies they were sometimes being adopted quicker than they could be proved effective. What do you think about that evidence? Do you think there is a case for that or not?

Marek Rejman-Greene: I think we have to separate the commercial sector from the state sector. The commercial sector has its own drivers. Whether or not they wish to use the technology as a security system or a convenience service is their commercial decision. In the state service there has generally been a reluctance to go straight through and be one of the early adopters, perhaps with the exception of automated passport gates at airports. We were the second country in the world to go for those gates because we saw the potential. We had to live with all the development and we are now into the third generation of those gates. We do not necessarily have to be the first in the field. Many of the large-scale systems are already trialled and tested in other countries. We have the benefit of going to those countries and understanding how they work, and what the benefits and costs are.

Q150 Stephen Mosley: I am conscious that we have not heard from the Minister on the issue of scientific advice on biometrics. From the ministerial chair, how effective is the scientific advice that you receive?

Lord Bates: It is very effective in formulating the response—the advice which comes up to Ministers. In all these things, particularly at the present time, I am slightly suspicious

when people claim almost oracle-like knowledge and expertise. Therefore, I think that the approach which has been outlined is the right one: rather than believing that you have the answers, you engage in what you might call open source—not quite cloud, but that type of thing—and say, “This is very fast moving,” and you look at what other people have got. From that point of view, the Government position is that we very much approve of working with European partners in particular, where we have some ongoing projects to develop things and learn the technology internationally. Close relationships with the United States are very important, particularly from the security point of view, and information is provided there. Rather than trying to have everything in-house, drawing from a wide range of academic expertise and practice is the right approach, and so far it seems to be serving us well.

Q151 Stephen Metcalfe: I think you were here for the first panel. Is that right?

Lord Bates: Yes.

Q152 Stephen Metcalfe: You heard some of our discussions about the police use of facial recognition software. When did the Home Office become aware that the police were developing a searchable database, and were you involved at the outset? There is some confusion about whether it is or is not being used.

Lord Bates: As to the precise date, I may need to write to you so that we get the facts absolutely right. Chief Constable Sims referred to the police national database being brought into the Home Office. Facial data was put on there, and it was a searchable database. At that point, you rightly identified in your line of questioning a gap, which we recognise, in the analysis, and the safeguarding of public trust and confidence in how facial recognition data is used, because the technology is moving at such a rapid rate. Now is clearly the point when we need to look very carefully at that. In the light of the court ruling on the Met police’s retention of it, the Home Office instituted a policy review of the statutory basis for the retention of facial images. That will take place and we will be consulting key stakeholders. We would also welcome the views of your Committee on what safeguards need to be there.

Q153 Stephen Metcalfe: I do not want to put words into your mouth, but I think what you have just said is that you became aware of this rather than being involved at the outset.

Lord Bates: I need some technical help on that. There are two elements. Clearly the collection of facial images has happened for a very long time, and it is an accepted process. What we have not necessarily had before is the software technology to be able to search that on the computer, and therefore the question of whose facial images should be on it has come to the fore.

Marek Rejman-Greene: Perhaps I could help on that point. In about 2012, a supplier—the integrator that provides PND—demonstrated the capability to Chief Constable Mike Barton and the rest of that team. That sowed the potential for the use of facial comparison

in PND. It was only this year that the capability was switched on. It went through a rather long period of time, and I believe the gradual uploading of images was done this year, but I need to confirm that.

Q154 Stephen Metcalfe: It was demonstrated to the Home Office first.

Marek Rejman-Greene: To Chief Constable Mike Barton; I think we were not directly involved in that demonstration.

Q155 Stephen Metcalfe: It was demonstrated to the chief constable that this—it is PND, isn't it?

Marek Rejman-Greene: Yes.

Stephen Metcalfe: The capability was there and then it was switched on. What I am trying to get to is: at what point did the Home Office think there might be an issue that we need to regulate? We are now searching through photographs for people potentially to interview or request information from, and there is a privacy issue. If we do not know how stable and how good that software is in finding the right person, we may be infringing someone's privacy. I want to know at what point you became aware of that, and what steps are being taken to address it.

Lord Bates: The permanent secretary at the Home Office expressed a concern about this. He has acknowledged that there should have been better consultation between the point at which you have the images and the point at which you flip the switch, effectively, to enable that database to be searched. There should have been more consultation at that point. In relation to the retention of images, particularly by the Met, I think it would be fair to say that the permanent secretary expressed some disappointment in writing in July this year to the Metropolitan police that they had not dealt with the issue as expeditiously as he would have liked. We are moving further down that track; it is changing almost by the week.

Q156 Stephen Metcalfe: Putting aside the time line, do you think that in principle it is right that people who have not been subsequently charged or convicted of crimes should have their facial features searched for potential links? Is it proportionate?

Lord Bates: You use the word "proportionate", which is a key test in this. We have to acknowledge—I am conscious that I am not directly answering your question, and I will explain why. I am very conscious that if you look at other data that was being held—DNA data and fingerprint data—the information commissioner and the biometrics commissioner said that, if there was no charge, it must be destroyed, and millions of records have been destroyed. Following that principle across, there is certainly a big question, and the reason why I cannot say at this stage is that to do so would be to pre-empt the review I have just announced to consult people on what should be the correct response.

Q157 Pamela Nash: I was surprised to learn during the course of this inquiry that the Biometrics Commissioner's responsibilities are confined to DNA and fingerprints. He made it very clear this morning that he does not want to expand those responsibilities and his work load. Have the Government considered extending the responsibilities of the biometrics commissioner to include all biometrics that are used by the police force?

Lord Bates: Of course we are always open to review on the powers. I was listening very carefully to what the Biometrics Commissioner was saying this morning.

Q158 Pamela Nash: Just to warn you, he is behind you.

Lord Bates: Is he? It sounds like a Christmas pantomime.

Q159 Chair: On this question, there are lots of images that Members of Parliament would like deleted.

Lord Bates: Not least from Select Committees.

Of course we are going to look at this. We had taken the view, until we commissioned the review I mentioned in answering Mr Metcalfe's point, that we felt broadly that they were adequate. We have heard what the biometrics commissioner said, and we have launched the review. I can say to the Committee that the role of the biometrics commissioner in response to facial images will be a key aspect of the review.

Q160 Pamela Nash: Would the review also consider, if it felt it was inappropriate, whether there would be other methods for that to be regulated? If it becomes clear that it should not be the role of the Biometrics Commissioner, or that it would be too much for that office, would there be further consideration of who should have responsibility for these additional biometrics?

Lord Bates: Yes. We recognise that the current governance of the data being held is not sufficiently covered. The chief constable, the police and the Home Office recognise that. That is the reason why we need the review. We are talking about different elements in terms of facial recognition, and there are limitations in the science of it. Facial recognition, unlike DNA and fingerprints, can change over time, particularly in the case of young people. Today, the Home Secretary and the Prime Minister are announcing very important developments in child exploitation identification software online. That technology is of a different nature from a fingerprint, an iris and DNA. Therefore, there could be an argument, which will be made in the review, that they ought to be treated in some way differently.

Q161 Pamela Nash: I think we can appreciate that, but it is a fair prediction that the technology is advancing rapidly and might be used further in the near future by the police and beyond. Have the Government considered in the review who will be responsible for new technologies—perhaps ones we have not thought of yet? How can we frame legislation and policy around the new technologies that will be emerging in the future?

Lord Bates: On the technologies, perhaps I could bring in my colleague. I will then deal with the policy side.

Marek Rejman-Greene: Chief Constable Sims mentioned the potential use of speaker recognition. Other technologies in the last few years have been interesting—for example, the potential to use gait recognition from CCTV, and trying to infer. That area is almost straying into the forensic science regulator's domain. In the last few months of the previous forensic science regulator's time, I think he was beginning to try to get various sectors to regulate their own areas. In a sense, the forensic aspects were being taken care of. As to where police would do it, I think Chief Constable Sims said there is an interest in trying to make the most use of current technology, rather than perhaps branching out to ever more esoteric ones. Even though the potential may be there, the indications are that certainly for widespread police use—

Q162 Chair: Isn't this a classic area where, because you and I have limited powers to predict the future, it would be sensible to create a regulatory structure around the broader societal principles we are seeking to address, rather than specific technologies?

Marek Rejman-Greene: I think that is more a policy question than something in which I would be involved.

Q163 Chair: I would have thought that technologists would agree with the logic of that policy position.

Lord Bates: From a policy point of view, the broad principle of what you are saying is right. Whatever happens, whether it is gait—the way someone walks—or whether it is voice or face, whatever means we use to identify people, that seems to be pretty sensible.

Q164 Chair: It would seem sensible to pre-empt all of that by having a regulatory structure which said that if the police or any other agency were seeking to use evolving technology, it automatically slotted into the responsibility of an existing regulator rather than waiting until after the event.

Lord Bates: Chair, I appreciate your generosity in trying to phrase it for me, but I think we are more or less in the same area. I think the principles-based approach is the right one in fast-moving technology. That is the reason why we still have a Data Protection Act which does its job, even though it was enacted in 1998 and technology has moved on quite dramatically since then. We need principles and infrastructure which capture the broad

principles and give confidence, and therefore other new technologies can slip into them as they are developed. But that is a view, and we are open to further advice on it.

Q165 Pamela Nash: We are aware that the Biometrics Commissioner is responsible for the retention and use of biometrics by the police, but not the immigration database. Is that being considered in the review, or is it outside it?

Lord Bates: On that specific point, I may need to write to the Committee.

Pamela Nash: Thank you.

Q166 Mr Heath: You have said several times that you deal with these biometric matters on a cross-Government basis, so I am hoping that you will be able to shed some light on something that is not directly a Home Office matter—the Government identity assurance scheme which is being brought out. One of the assurance levels the Cabinet Office has indicated is biometric information. Of the 25 exemplar services that are being trialled, how many use biometric evidence?

Marek Rejman-Greene: None, because the infrastructure has not been put in place as part of the IDA scheme. As far as I know, all the services are at level two, which is quite a way short of level four.

Q167 Mr Heath: Do you know what the intention is in terms of bringing things up to level four? Is it that none of those 25 will ever be used at level four, or will some of them in due course, or are we talking about other services that would require level four?

Marek Rejman-Greene: The point is that the levels of assurance are related to the risk involved. When there is life and death involved, obviously we might be thinking about level four, but when there are just matters of relatively low levels of financial loss to Government, the decision was made to go to that lower level of assurance. It is a matter of taking the risk and understanding what appropriate security mechanisms are required.

Q168 Mr Heath: In your modelling of how it might be applied in circumstances where a level four assurance was necessary, is part of the thinking that there would always be at least some human involvement in the process, so you do not have complete automaticity? The exercise of judgment and a brain are involved.

Marek Rejman-Greene: Our present-day knowledge about the way biometrics systems work is that they are never perfect, so there will always be some need for and recourse to a fallback anyway. If you were to imply that there was an automated decision that affected the individual, it might well be counter to one of the Data Protection Act requirements, which is that you should not take that decision in a purely automated way.

Q169 Mr Heath: That is built into it.

Marek Rejman-Greene: I do not know. I cannot speak to it, because the plans for the much longer term of the identity assurance scheme are still being worked on. There is a lot of effort being made to try to get today's technology implemented.

Mr Heath: You have been very helpful. Thank you.

Q170 Graham Stringer: If I can take you back to the questions Andrew asked a few minutes ago, you gave a partial response. As biometric technologies change, are invented and develop, do you think it is necessary to review the data protection legislation?

Lord Bates: That probably relates back to what I was saying. Because it is principle-based, it has stood the test of time. The criteria used for assessing sensitive personal data, for example, are very clearly set out in the Act, and the different treatments of the two. I think it does hold firm in general. However, the statutory basis for facial images needs to be reviewed, and I have approved that work. It may be that the review shows a need for new legislation, perhaps relating to the Protection of Freedoms Act. It might be more that area that we look at, if needed, than the data protection.

Q171 Graham Stringer: To be clear, are you saying there are some specific reviews under way but not a general review of the Data Protection Act?

Lord Bates: The review which is under way is on facial recognition—how that is covered by existing legislation and existing governance through the commissioner's office, and also how it is supervised within the Home Office in the context of the police national computer. That is the scope of the review we are looking at.¹

Q172 Graham Stringer: You do not believe that a general review is necessary at the present time.

Lord Bates: We have not found that, but we are open to it. For example, I note the Committee's report published previously that looked at the responsible use of data, which we are in the process of responding to. That made some very interesting recommendations about privacy, the amount of data people share and whether they should be better aware of what they are signing up to. This is ongoing, and we will continue to look at it.

Q173 Graham Stringer: Are you completely confident that the current legislation protects citizens against biometric data being used in a way that they have not given their consent to?

Lord Bates: It would be difficult for any Home Office Minister to sit before a Committee and say they had absolute confidence in it. History tells me that probably the next day you

¹ The witness later clarified that, he intended to say "... in the context of the police national database."

wake up to headlines showing that your confidence was somewhat misplaced. The best you can do is to say you are sceptical, and keep it under a watchful eye and under review. We are looking particularly at areas like the operation of privacy impact assessments, the information commissioner's powers of investigation, and the sanctions he has available under the Data Protection Act. These are the kinds of areas currently under review.

Q174 Graham Stringer: Perhaps I can ask the question in a less minatory way. Do you have any evidence that biometric data have been used when people have not given their consent?

Lord Bates: I think that is the facial images case that we are currently wrestling with.

Q175 Graham Stringer: That is the only area.

Marek Rejman-Greene: There is probably also a case under the Protection of Freedoms Act where children's biometrics have been taken without any statutory measures.

Q176 Chair: This was in schools.

Marek Rejman-Greene: Yes. That is an example where the need for a specific regime has been recognised.

Q177 Graham Stringer: There has been some criticism that the Government have not been proactive enough in influencing data protection at European level. How do you respond to that accusation?

Lord Bates: It is certainly not what is happening on the ground. The operation that we have across Europe is very active. There is an agreement on sharing biometric data across Europe, which goes under the heading of "Prüm"—that is not an acronym, but the town in Germany where the conference took place. The Government have said they will look at that and we are preparing a business case on it. We are trialling some of the recommendations from that. We will make a decision on whether to join that set of regulations and directives in 2015, but, before that, Parliament will of course have its say, because it will require legislation to do so.

Q178 Stephen Mosley: In the written evidence we received from the Home Office it was stated that biometric identification systems should demonstrate "a lawful purpose, a pressing need and proportionality". How do you ensure that biometric systems demonstrate those three criteria?

Lord Bates: That is an excellent question. I will bring in my colleague to respond to some of the technical elements. It is something where we are aided by the independent offices of

the biometrics and information commissioners, the science advisers within the Home Office and a science council, which is chaired by the permanent secretary. Through those mechanisms we keep things under review, but it is in the nature of the fast-moving changes I have referred to a number of times that you are often reacting to particular stories, concerns and issues that come to light in the public square. You are reacting to them and examining them on that basis, and sometimes it is very difficult to get out in front. That is probably part of the thinking behind the wider strategy across Government and whether there is a need for it.

Marek Rejman-Greene: To expand on that a little, privacy impact assessments are made to understand what the trade-offs are. In the nature of those privacy impact assessments, you have a consultation process which enables all sides to bring to the fore their concerns and the opportunities generated by a new service that is perhaps under consideration.

There is also an economic angle to all of this. The business cases go through quite rigorous assessments to see whether there is a benefit as opposed to the costs involved in working on proposed new systems. There are those two technical controls. There is also the political dimension. That ensures that when information about this is published, for example, a proposed intention to go to tender, MPs—the political process—can engage to put the question: is this a proportionate and transparent way of introducing a new service?

Q179 Stephen Mosley: Do you think that open standards for the governance of biometrics are a suitable way of governing how biometrics are used within the commercial and Government sectors, or do you need a more formal legislative framework?

Marek Rejman-Greene: I think we have to separate those two. Obviously there are limitations to what we can do in terms of trying to impose standards on the commercial sector. They have to make a decision whether it is worth their while having an open system or one which is de facto their own, keeping all the information about how they implement a system within their own companies.

In terms of government systems, the first direction is almost always to try to look at open standards for a number of reasons, principally because it means that the services and systems are not necessarily custom-designed, so you can open it out to the marketplace and there is no need to have any hidden interfaces. It also opens up those interfaces to the sharing of data with other countries and systems, provided that is legal. Having open standards also enables all the details of how those systems operate to be out in the open. It allows for innovation, so you know the constraints within which to innovate; and it means, therefore, that UK companies can bid for parts of the systems that relate to the biometric component. I hope that has given you an idea.

Q180 Stephen Mosley: Yes. It sounds like the right thing to do. The follow-up question to that is: what are you doing to promote those open standards and encourage people to use them?

Lord Bates: We promote open standards for exactly those reasons through a myriad of international standards organisations—the WTO and many international groups. The main

reason why we want open standards is that biometric data is connected with travel, cross-border crime, protection and security, so it makes sense to do that. But there is that element, which seems to me quite right, that if a commercial organisation says, “Forget about the standards. We believe this one works best for us and we want to take a chance on it,” as a commercial organisation they should be able to do that. Government has to operate to a different set, as has been said.

Q181 Chair: I tend to agree with you that technical standards are not the bailiwick of Government; that is for expert panels in industry, the BSI and so on. One aspect of open standards which is hugely important is public confidence in them. If people have doubts about the integrity of systems, they can openly challenge if they know how the systems are designed to operate.

Finally, I want to move to maintaining public confidence in this whole space. We have to strike a balance between the needs of law enforcement and other agencies, and the necessary protections of privacy when it comes to biometrics. What are you doing to try to maintain a sensible balance in that space?

Lord Bates: We want to make people aware of what rights they have, the access they have, and the people who operate on their behalf. We were talking about the commissioners’ offices and getting people to believe that, if they have a grievance and concern, they can go there and there is an appeal or a redress mechanism available to them. There is also the work of Parliament. I suppose that ultimately—which is where your Committee is going—the more we get science and technology out there and debated in the public square, the better it will be, because that plays into almost where we began with this process: this careful balance, which is not just one for politicians, Home Office Ministers or officials. It is for society as a whole to say, “We are aware of the significant advantages of keeping us secure, keeping our borders safe, keeping our loved ones safe, and also the attractions of technology in providing ease of access and movement, and also in economics and commerce.” But there have to be serious concerns about the potential risks of having such data held, its proper use and how you maintain that debate. The more discussion and the more awareness there is, the better. The Government are looking at ways to do that, but it is only a part of the discussion. This is something in which the media and civil society need to engage and have a far wider debate about the issues.

Q182 Chair: Stemming from that, Sarah Newton asked the previous panel about the security of the data. Industry has said to us that often the security aspects of this are bolted on at the end rather than being an integral part of design. Can we have an assurance that any system that Government procure, or authorise procurement of, will have security of people’s data right at the heart of it?

Lord Bates: From my experience and the discussions I have had on this, it seems as if it is always the private sector that might bolt on security at the end of the process. It seems to me that Government in particular bolts on security right at the beginning of the process. It is quite interesting to see different public attitudes. People willingly share quite detailed information about themselves on websites and social media without much care or concern.

When that same information is provided to the Government there is a different set of criteria, yet actually security is probably far more hard-wired into every process of what Government does, particularly because it is dealing with national security issues, and I think people could have more confidence in that particular area of security of data. The private sector probably has some catching up to do.

Q183 Graham Stringer: Can I ask a very similar question to Andrew's but perhaps take a step back? We have all this wonderful new technology at the moment that enables the police to do things they could only have dreamt of 25 years ago, and we have proper concern about balancing that against individual privacy and personal rights. When you step back and look at the breadth of the legislation, do you think we have got the balance right, or that, as the *Daily Mail* and other newspapers think, because of the concern about privacy and some of the inadequacies of the security systems, there are rapists and murderers going free because we have destroyed part of the databases, and possibly we are not going to keep the data that we have got? Do you think you have the balance right throughout all the legislation?

Lord Bates: It is a very good question, and it is almost a philosophical one.

Q184 Graham Stringer: It is a very practical question as well.

Lord Bates: If we have the balance right, I would say it is a fine balance in this context. The database provides the police with over 25,000 matches a year, and 700 matches to murders, manslaughter and rapes. We recognise that that is where it is doing its job very effectively. On the other hand, we are having a discussion about facial images held by the Met police. Those are the two ends we balance, but I think it is right. The best you can hope for is that Parliament, the Home Office and the systems of government hold decision makers' heels to the fire over this to get them constantly to think, "What is that balance? Have we got it absolutely right?" because it will shift over time.

Q185 Graham Stringer: Do you think we have got it right? I suppose that is the question I was asking.

Lord Bates: We have broadly got it right, but it is not quite there as of today in relation to facial imagery in terms of the overall strategy. That is the reason why we are undertaking the work to correct it, if it needs to be.

Chair: Gentlemen, thank you very much for your attendance this morning. It has been really interesting.