HOUSE OF COMMONS

Science and Technology Committee

Oral evidence: Current and future uses of biometric data and technologies, HC 734

Wednesday 26 November 2014

Ordered by the House of Commons to be published on 26 November 2014.

Written evidence from witnesses:

- Biometrics Institute
- Professor Louise Amoore
- Professor Sue Black
- Identity Assurance Systems
- 3M
- Northrop Grumman
- Innovate UK
- Big Brother Watch
- British Standards Institution

Watch the meeting

Members present: Andrew Miller (Chair); Jim Dowd; Stephen Metcalfe; Stephen Mosley; Pamela Nash; David Tredinnick

Questions 1-81

Witnesses: **Professor Juliet Lodge**, Emeritus Professor of European Studies, University of Leeds, and member of the Privacy and Policy Expert Group at the Biometrics Institute, **Professor Louise Amoore**, Professor of Political Geography, Durham University, and **Professor Sue Black**, Director, Centre for Anatomy and Human Identification, University of Dundee, gave evidence.

Q1 Chair: I welcome our panel here this morning. We do not normally refer to the people in the Gallery, but I give a particular welcome to the observers who are involved in the Royal Society pairing scheme.

This short inquiry that we are undertaking relates to biometric systems. It is interesting that a couple of weeks ago I was privileged to be at the Barclays technology centre. The privilege was being on a platform with a 93-year-old who had worked at Bletchley Park, and we played with an Enigma machine. While looking around at some of the technologies there, it is fairly obvious that the banks are researching some advanced biometrics.

First, I ask the three witnesses to introduce themselves and to explain why we have not seen the widespread adoption of biometric systems in the UK.

Professor Amoore: Good morning. I am Louise Amoore, professor of geography at Durham university. My perspective on take-up is that we tend to think of it in terms of first-generation biometrics. We tend to think perhaps of national identity card-type schemes—the Heathrow trials of iris or miSense, for example. We might then conclude low take-up, but my feeling is that what we are seeing is a huge expansion in more passive forms of take-up. For example, many of us may not imagine, as we upload our images to Facebook or Twitter, that an algorithm is being used to extract biometric data from those images. If we are willing to think about biometrics in those more expansive terms, I would say that there is now an indirect take-up and one that could see these kinds of techniques becoming ubiquitous.

Professor Lodge: Good morning. I am Juliet Lodge. I am an academic who has been working in this field for 16 years, but I am here representing the Biometrics Institute, which was founded in 2001 in Australia. It has a branch here, and it prepared the first privacy code, which was adopted in the early part of this decade. It is also very much concerned with the impact of privacy. The members of the Institute are drawn from all different areas—industry, Government and commerce, those who use identity management, such as airports and for border control purposes, and academia.

The emphasis that we have on biometrics corresponds to what has already been said, in the sense that we believe there is a much wider incidental take-up of biometrics, apart from the use of biometrics for accessing services, such as accessing travel, banks, finance, perhaps accessing one's driving licence and insurance, and all the things that go along with social media.

The other area where there is much more in terms of potential uptake for biometrics is in the area of e-health and implants, which also affect the way in which people behave. From the perspective of the Biometrics Institute, it is a question of biometrics being not defined in such a narrow way that we only think about it as a biometric token embedded in a document that allows one to access a certain space. Therefore, from our perspective, I would say that the uptake of biometrics is increasing. It is vast, but the real issue is to ensure that it is done in a way that is responsible, transparent and accountable, reliable, secure and robust, and in a way that is going to be acceptable to the public, who so far have not been terribly well informed about what a biometric is or how we can use biometrics.

Professor Black: Good morning. I am Professor Sue Black from the University of Dundee. I am a forensic scientist, and my particular area of interest is looking at the translation that we have of biometrics from the security industry into the courtrooms. I wonder whether part of the lack of uptake is about an element of faith and trust.

Unfortunately, a lot of the public watch our dreadful "CSI"-type programmes, and we have an element of distrust—that your fingerprints will be used in a way that is inappropriate and nefarious—and we all know from "CSI" that you can get everything you could possibly ever want from a drop of DNA. We have an element of the public perhaps not fully understanding the remit and extent of biometrics, and we have a fear and a trust element that is partly a result of the courts but also this forensic awareness.

Q2 Chair: Do I take it from those three answers that none of you sees some game-changing application that will suddenly set the world alight and that all will change? It will be an evolutionary process by which we adopt these technologies.

Professor Lodge: There is an issue around the casual adoption of biometrics.

Q3 Chair: There are some points about the disadvantages of that, but I am asking specifically whether or not you are expecting to see some game-changing application emerge.

Professor Lodge: It depends how they are used and in what context. What does one mean by game change? Do we mean that suddenly everybody will be using biometrics in order to access everything—one biometric that is going to allow interoperable access to services in exchange for information—or does one mean something different, a specific application that is going to lead to vast commercial growth in a specific area? I am a little unclear about that.

Professor Amoore: Perhaps there are game-changing technologies that we need to think about, but they are around what we call advanced analytics. It is perhaps less about the availability of biometric data and more about our capacity to read that data. I could provide the Committee with some examples afterwards, if that would be useful, in terms of written case studies.

There are analytics engines, for example, that can mine biometric data that is available on the internet, and link that to other forms of data. It is a game-changer to the extent that we are then thinking not just about the biometric data but what they are linked to. That moves us more in the direction of indicating not just who someone is but suggesting that one might be able to infer someone's intent from some of the biometric data—gait recognition technologies and so on. While there might not be a single game-changing technology, there are significant changes that we might want to think about.

Professor Black: If you look at forensic science, the last real paradigm shift—the real game-changer for us—was 30 years ago when we starting bringing DNA into the courtrooms. There has been no game-changer event. Surely, we are ready for one now. There must be something that is going to change that, because we have got to a point with DNA where it is starting to be looked at a bit more carefully in the courts. We have had a couple of cases in Australia where the DNA has been rejected by the court because it has become so sensitive, so complex, that we have almost researched everything that we can out of that DNA application. We need to move on to something else, but we do not know what it is yet.

Q4 Chair: Professor Lodge, I started my remarks by referring to banking. It seems to me that if our banking system were to adopt a particular technology—let's be very simple—and insist that your photograph has to be on your credit card, which would be a nice simple one, if it were insisted upon, it would happen. It would sweep across the country rather quickly, would it not?

Professor Lodge: Yes, in the sense that it has been adopted in a number of other countries, where they combine fingerprint or vein recognition with voiceprints and a facial image. The real issue for the widespread adoption for access control—I still see it as part of access control rather than the analytics—is that it opens a huge potential to be exploited. There will be game changes in the area of e-health, because of the way in which robotic implants can affect behaviour for good or for ill, and where you will have questions of liability if there are failures.

The real issue around e-identity for access control and the linkability is this. The example that you have given is purpose-specific. So you can have very limited purpose and you can minimise the amount of information; you can decide whether that is going to be transferable out of those banking arrangements to other banks and who is going to be able to access it. That sort of thing is somewhat different from the other types, and it relies on a high degree of trust.

Trust and accountability is what is problematic, because there has been research that has shown that people would rather the banks looked after their identities than the Government. Similarly, if trust in banks fell, people would begin to think that some of the social media people might be the ones to manage their identities. However, this is all very ephemeral and transient, and one has to think about the sustainability of who is managing these tiny tokens that are supposed to be a representation of someone's claim to be who they say they are.

Q5 David Tredinnick: Good morning. Some of my questions will cover partly what has already been discussed.

What evidence do you have that public acceptability of biometric technologies is resting "on a knife edge"? Putting it another way, how finely balanced is public opinion in favour of or against biometric technology?

Professor Amoore: It is extraordinarily difficult to make judgments about public opinion. Usually when you see these kinds of surveys, the kinds of questions that are asked are, "Would people be satisfied with the submission of this biometric in return, for example, for greater border security or for greater integrity in terms of their identity—identity theft protection?" One of the difficulties with making assumptions about public acceptability is that we tend to tie the biometric to a promise and that promise is not necessarily deliverable. What gets lost in that public debate is that it is a probabilistic science, and it is never going to offer complete border security or complete protection from identity theft.

I would need to be more convinced about the way those questions are asked of the public. Something very specific would need to come out, and that would be the extent to which biometric technologies are now about automated recognition. That is an area where there

needs to be greater public debate about the relationship between machine recognition, algorithmic decisions and the intervention of a human person.

That is a matter also for the Government, of course. Where we see electronic borders and automated border controls, the promise is that you can have 10 automated gates reading your biometric chip and your passport, supervised by a control room, or by one border guard instead of 10 border guards; that promise is being made about security on lots of levels. The question is whether trust in the biometric would involve some understanding of the role that biometrics play in that broader system.

Q6 David Tredinnick: I have been through the new terminal 2 at Heathrow, which was a wonderful experience because it was so fast. That is because of the biometric screening, which is on the positive side.

What sort of impact do you think is made on public opinion by stories such as the one in the papers last week of Russian hackers being able to view home security videos of somebody in their own bathroom? What sort of impact do you think that has on public opinion, and do you have any suggestions as to what can be done about it?

Professor Black: That is a very big question.

David Tredinnick: It is a difficult question. It may be an impossible question, but we are here to ask questions.

Professor Black: It is about fear.

Q7 David Tredinnick: People are worried and frightened.

Professor Black: They are frightened. One's security, one's identity, is one of the things that people probably hold most dear to themselves, because it is the representation of self. The willingness to hand that over and entrust it to somebody also has the implication that there will be others who will not be trustworthy but who will want to enter into that space that you have. Every time we have media scare stories, true or otherwise, they chip away at the public confidence in our ability to hold our identity secure and who we are going to trust to hold it. It is very much about trust and fear.

Q8 David Tredinnick: The problem is that the absolutely trustworthy organisations that we believe in are absolutely trustworthy until they are hacked.

Professor Black: Yes.

Q9 David Tredinnick: I have spoken to one colleague this week, who is on a very sensitive Committee, which involves passing information to other people. He is not using e-mails; he is using the post. I put it to you that we have reached a point now where we are going to have to go back to the past to get security, because there is no security with Governments hacking into systems.

Professor Lodge: This comes back to the earlier point that there has to be trust in the technology. There has to be trust in the biometric application. There has to be trust in the procedures that are used for transferring the data or reading the data, which may be the weakest link in the chain, and the way in which the data is handled. You spoke about public trust. Any breach in any of those little areas is going to have far more of an effect on the public belief in the system than one might expect.

The other thing is to make sure that people do not think that the biometric is foolproof. It is not foolproof. It may induce convenience, speed and efficiency gains, but it does not necessarily produce the high degree of certainty displayed.

Q10 David Tredinnick: Do we then have to divide or categorise the safety of others? We can use it for border control, where you have a supervisor; it is a great aid there. But there are some things that it cannot be used for satisfactorily. Is it not part of the problem that we are not properly differentiating the risk levels?

I do not want to occupy all of the Committee's time, but I have one other question to add to that. What efforts do you think the Government have made to engage with the public about biometrics since the ID scheme was scrapped in 2010? Do you think that the Government have been engaging properly with the public since its scrapping, which some would call a fiasco?

Professor Lodge: No.

Q11 David Tredinnick: Would you expand on that, please?

Professor Lodge: There is a little bit that is done through the introduction of biometrics in schools, where people frequently do not have the choice. In theory, they have a choice as to whether the children provide a fingerprint for registration, library books and payments. They know a little bit around that, but they do not necessarily make the inference that it is about electronic ID management.

Professor Black: I go back to your point about whether we have to go back in time. The answer is that probably we do. If we are moving so fast that we are running to meet commercial needs and security needs, have we forgotten the scientific base line? I wonder how much core science we still have to go back to and look at. If we do not do it now, will we ever do it? We run the risk perhaps of failure at a later date, when we ought now to go back and look at the foundation. Now that we understand the market better, do we need to go back and give it a stronger foundation? You are right in that respect.

Q12 Stephen Mosley: In your two previous answers to both the questioners, you talked about trust. I want to focus on trust in the technology. As a panel, do you consider that the matching algorithms in the biometric systems being used at the moment are scientifically robust and effective?

Professor Amoore: In terms of thinking about the science of biometrics, this is one of the things that we have looked at closely in our research. We have tried to follow through the

pathway from the writing of an algorithm, from that level of science, which is often done by physics and mathematics graduates, through to how that technology becomes part of a broader solution or system.

We have noticed that, at the level of the writing of codes, at the level of looking at extraction algorithms and matching algorithms, they are quite candid about it: "This is probabilistic. You will have to speak with the people who are buying the system, to ask what the threshold will be, what sort of tolerance they have for the false acceptance rate versus the false reject rate, and so on." Then something happens in that debate, which does have a foundation in terms of thinking about the multiple sciences involved in biometrics, through physics to biological sciences and so on; it becomes lost at the point where we see a large commercial solution, which is often sold off the shelf for different sorts of techniques.

The one useful thing that we could do is to go back and say, "Are there ways of thinking about how the doubt in the science is present in the room when they are looking at the screen and writing the code, but that is lost by the time it is part of the hardware technology being used, perhaps for CCTV or managing football stadiums or border controls?" It is important to disaggregate the science of the algorithm from the solution as it becomes part of a broader picture.

Professor Lodge: You could have an extremely accurate algorithm for the match, yet the way in which it is introduced into applications can then weaken the security that you attach to the answer that you get from the match on match. The applications for handling and so on are extremely important and can undo the good intent that may lie behind an algorithm written for a specific purpose.

Q13 Stephen Mosley: Is there any expertise or any organisation that does professional independent testing of the final products?

Professor Lodge: The Biometrics Institute has a vulnerability assessment tool, which is a way of looking at how robust the system is against spoofing attacks, but I am not aware of an organisation that would take every single application that is potentially on the market at the moment and say that it is the most reliable in terms of a specific criterion.

Professor Amoore: It may be worse than that. To a certain extent, those involved in the earlier section of the system often do not have access beyond the test data when looking at how it is running, and they are often open about it having a five-year life span, in terms of the model degrading over time, or the particular conditions of ambient lighting, for example, that were involved in facial recognition for the trials that I talked about earlier. Even to think about it on what grounds you would then validate it in the lifecycle of the application, whatever it is, is missing at the moment.

Professor Black: The testing for me comes in the probative within the courtroom, and the only biometrics that have got into court in terms of thresholds of admissibility are DNA and fingerprints. Fingerprints are being challenged. A key case north of the border showed that it was not the biometric that was at fault but the way in which we analysed the biometric. We have to keep going back to these techniques and these approaches, and we

have to keep justifying them and validating them. It is extremely important that we do not get to a level of complacency.

Q14 Pamela Nash: In the written evidence that you provided to the Committee prior to this session this morning, you indicated that you did not think that current legislation on biometric data was fit for purpose. Would you expand on that? Do you think that the Data Protection Act could be changed or amended in order to cope with the advances that have been made, or do you think that it requires a whole new outlook?

Professor Black: It possibly requires a whole new outlook. Given the way in which biometrics is changing in our society, it is running ahead of our capability to manage it. One of the research projects that we have been looking at is the relationship between your physical identity and your cyber identity, because the crossroads into the two is extremely important. While we have measures of looking at our cyber identity and measures for our physical identity, getting across that barrier to the two is an area of no man's land, where we really do not know how we are going to connect one to the other.

In our research project, all of our participants gave their ethical approval to having their images taken, but they could not know what we were going to find at the end of our project. We now have connections. If they had known that those connections existed, would they have been prepared to give us their photographs to be able to do that? We now have an ethical quandary. They have given us permission, but did they know what they were giving their permission for? That is because the science keeps moving it forward and keeps changing it.

We are behind, and this is an important time to ensure that we do exactly as suggested—that we go back and come forward, and go back and come forward. It is a retest all the time, to ensure that we are on the right path. For legislation, it is time to go back, reassess the base line and move on.

Q15 Pamela Nash: I appreciate that we are the legislators and that it will be a question for us, but do you think that it is possible? What you are asking us to do is to legislate for the future. Do you think that is possible for us to do, with the correct advice?

Professor Black: No, it is not possible to legislate for the future, but I hope that it is possible to legislate for possibility—for change, for a degree of flexibility—while retaining an element of strength and control. It is an ever-moving market, and it is going to keep moving, and moving faster. We have to be careful that we do not end up with legislation that holds this back, because we have written it in such a way that it is only for the current time and that does not give it the flexibility to cope with the advances ahead of us.

Q16 Pamela Nash: Professor Amoore, you had similar concerns in your evidence.

Professor Amoore: Yes, I did. It would be a step forward for us to begin to think about all biometric data in a broad definition, to include tagging in social media and so on. I would say that it all ought to be considered as sensitive personal data. In a sense, it would mean

that we could think about that in terms of existing law, because different rules apply to processing, storage and so on, when you think about sensitive personal data. As it currently stands, not all of that data are considered to be sensitive personal data, and it might be time for us to think about that.

Q17 Pamela Nash: Would you give us an example of what you think should be considered?

Professor Amoore: There is the possibility of linkage between, for example, tagged images, visiting websites, clickstream data that are analysed and transactions data, and this is very sophisticated in the commercial area. For example, Adidas has a system that it calls Consumer DNA; it is asking what the ideal future Adidas customer looks like. It is using YouTube videos, and it wants to know not just what this person likes to do, what music they like to listen to, what trainers they are likely to purchase, but it also wants to know when they are next present online. Part of that is knowing something about their biometric template from the facial biometric data.

The linkage to the biometric makes all sorts of things possible in terms of when this person appears again. It might be in an Adidas store or on the internet, so it is both the real and the virtual worlds. But, as Professor Black said, that means we have to rethink consent, and to what extent we can now reasonably say that someone has given their consent for that kind of questing to take place. We need to think again about consent, and we should think about all biometric data being considered as sensitive personal data because it can reveal things relating to race, ethnicity, sexual orientation and so on.

Q18 Pamela Nash: Do you think that it is possible for Governments to regulate for that commercial use of biometric data? Are there examples globally that we should be looking to for best practice?

Professor Lodge: One of the things that would help would be to take this more general view of biometrics, but we should also talk about the purpose of use, the repurposing, the unanticipated use, the outsourcing of that material or the handling of that material, which may not be in line with what was originally thought it was going to be used for. People become distrusting when they find that, for example, they went to Adidas and that information is used in a way for which they did not give consent.

It is an issue of looking at legislation in a much more holistic way so that one does not always separate data protection from a biometric ID card, from perhaps transactional, commercial or financial identification data, but one has an overarching framework that would take into account the legislation and regulations to which you have already signed up. It would take a more general view of how, in the age of an internet of things, where uploads may provide information to a mobile phone that is passing, this is going to be regulated. It requires a complete step change in the way in which we think about legislate in future.

Q19 Pamela Nash: I may ask a little more about that later. Are you saying that this could be legislated for by managing the data under an updated version of the current Data Protection Act, rather than it being treated separately?

Professor Lodge: To update it, and also to have a really thorough review of what it means in an age where devices that people use communicate imperceptibly with each other—invisibly.

Q20 Pamela Nash: In the last question, we were talking about legislation on the management of the data that are collected, but the technology is advancing quickly. Could we regulate that in a better way in the UK, or is it something that has to require international co-operation in order to legislate for future technologies?

Professor Lodge: It has to be international, doesn't it, because there is so much outsourcing and so many different players contribute to one application? We might outsource the handling of public data on driving licences to a particular company, which may not be based in any EU state subject to EU regulations on the handling of such data. From our experience in the Biometrics Institute, where you get dialogue between vendors, suppliers, developers, the scientists, industry, commerce and Government, that is a route towards creating the kind of guidelines that inform practices that are going to be accessible, to ensure that ethical behaviour is entrenched and that the individual is protected, along with their dignity.

Professor Black: When you enter into whatever the agreement is on your biometric, it is very local for you. You may be interacting with something that is on a national scale, but in reality most of what we do on a daily basis, if we interact with the internet, is on an international scale. The problem is global. It is not national or local; it is global. Overarching international legislation at some level is appropriate.

Professor Amoore: Part of the issue is also around how we think not only about public data but public money, particularly in the sorts of rules that apply to procurement, for example. One of the things that we have noticed in our research is the extent to which the large consultancies and the large IT organisations buy up small biometric start-ups. That is interesting because, when you have a Government procurement relationship, it is not directly with the people who have the small start-ups who are devising the biometrics; so it is more difficult to ask the questions. It is not only a case of the technology outpacing our vocabulary to ask questions about how it might affect our democracy or our society, or what the implications might be.

There is a gap between the development of these technologies, often by small cutting-edge innovative start-ups who are looking for new ways of using biometric data, but, as they become part of a large-scale solution like Accenture or IBM, how then do we ask those questions? What is the accountability in the relationship between the Government and the public, and the supplier of the technology? The technology is never a single thing; it is always part of this much bigger assembly that we need to think about.

Q21 Pamela Nash: That is why it is difficult.

Professor Amoore: Very difficult.

Q22 Chair: It strikes me that that may be very much applicable to the UK; but RSA, for example, grew out of a garage in the States into a fairly big business. The algorithms were originally developed at GCHQ here, and we were not smart enough to commercialise them.

Professor Amoore: Absolutely. One of the key elements is how the technology travels beyond its original design and usage. Some of the scientists involved in this are concerned about discovering that the algorithm that they wrote specifically for casino access has found its way into some other application. They found out by default that it is their model. It is probably impossible to legislate for that, but we could certainly think about the sorts of regulations that we have around procurement.

Q23 Stephen Metcalfe: I want to go back to the issue of linkage. Professor Amoore, you talked about some of the concerns that you have on linking biometric data with transactional behaviour data. Are there any upsides to that? Are there any benefits to linking those that add an extra layer of security?

Professor Amoore: Yes. It seems to me that the technologies that we see in social network analysis have seen some success. Professor Black might be able to talk about those in relation to child protection, but it is certainly not an entirely negative story. However, we need to be cognisant of the probabilistic nature of that as a technique.

Where you have incomplete fragments of data, some of it biometric data or behavioural data, and you link together those different fragments, what sort of threshold do you need to cross to make somebody subject, for example, to an automated decision? At what point would that automated decision lead to a human person intervening and investigating it further? The relationship between the social network analysis is very important, which can be done in an automated way, involving analytics and algorithmic technologies, but at some point there has to be a human intervention. That probably is something that we need to think about, because it is a probabilistic science, and because we can think about dealing with a world of uncertainties and certainties around internet online abuse or around terrorism, we might say that one needs to be able to make a decision under conditions of uncertainty.

Biometrics appear to lend a certainty to that picture. They appear to say that, if you can anchor your decision in the human body, you can have a degree of certainty about it. We need to think about some of the vulnerabilities in security when we do that. One example of that would be plans to make the screening element of security at airports risk based and linked to biometrics. At the moment, as you move through, you are almost an anonymous individual. You do not scan your passport at that point and your belongings are separate from you, so the people looking at the screen cannot make the connection. The idea is to submit the biometric again at that point so that the connection can be made. However, that will still be a risk-based technique, so we would be giving our consent to greater attention being given to the high-risk people than to the low-risk.

Of course, that again involves a probabilistic judgement about where you target your resources. Biometrics are often used to target resources in particular ways.

Professor Black: There are unquestionably benefits. A huge amount of the research in biometrics has involved the hand, because it is a part of the body that we are comfortable

to have scanned. If you go through security, depending on your ethnic background, it may be the only part of you that is available. There is a lot of research in relation to the hand. We have taken that and used it and involved it in the identification of perpetrators of child sexual abuse.

Being able to take the biometric, as Professor Amoore said, is about the probability. The only certainty we have is the certainty of exclusion, so we can say, "This is not." It is incredibly important for our courts that our biometrics can say, "This cannot possibly be." That is because it is an inherent biometric, a characteristic of your anatomical make-up. Whether you are the perpetrator does come down to probability and how strong is that probability. The translation of biometrics into other fields can be extremely positive.

About 82% of the cases that come to us from police forces end up in a change of plea. That change of plea is incredibly important for the courts because it saves a tremendous amount of money, but, much more importantly, you do not have a child having to go into court to give evidence against their father, their brother, their uncle or whoever it may be. There is a huge social benefit to it as well. It is very much about a balancing act between the benefits and the detractions.

Q24 Stephen Metcalfe: You talked about automated decision making. We are investigating how to make people more aware of this and how to regulate it without changing the benefits completely. You mentioned human interaction. Is the core of what a regulatory system should be, when you have linked data, that there has to be some human interaction before serious decisions are taken?

Professor Black: From the forensic aspect, yes, it is. While we can automate fingerprint detection, and we can automate the biometrics that we use on the hand, the final decision before we go into court is made by the expert, by the person who is trained to look at that data. As Professor Amoore said, at low level security, there may be no need for a personal intervention, but in areas where security is heightened, for whatever reasons, you may wish to introduce that extra tier. That is certainly what we would do in the courtroom.

Professor Lodge: There is one other element to bear in mind. You can have genuine breeder documents and genuine biometrics and create a genuine identity based on a false claim. It is not just the theft of genuine documents. If, for example, it is for the provision of a visa, at that point you must have somebody who is able to go through this, because any automated decision making is based on a bias that is written into it at the start.

Professor Amoore: There is already a legal basis. In the European Union data protection directive, article 15 is about protecting citizens from decisions made about them that have consequences for them, which are automated. The element of human intervention is also about acknowledging the fallibility of the system. In a sense, somebody needs to authorise that they can make that judgment on the basis of those particular criteria at that moment. I think that is important.

Professor Black: Personal intervention also gives an element of increased faith and trust—that you are not just relying on the machine to decide that you are who you say you are but

that somebody else is physically involved in that. If we have a fully automated system, we will have greater trust issues, but we do need to have personal intervention.

Q25 Stephen Metcalfe: I return to the issue of giving consent for your data, whether biometric, transactional or behavioural, to be shared, linked and used. Do you think that the public will ever get to the point where they understand the complexities of what they agreed to when they ticked that little box that says, "I agree"? How can we make that easier to understand?

Professor Black: You need first to ask the question of the scientist. You would ask a scientist, "Would you be prepared to give us our biometrics?" If the scientists are not prepared to give you the biometrics, where is the public confidence going to come from? We need to start right at the beginning.

Professor Lodge: There is a feeling that you do not have the choice. If you do not tick the box, you cannot access the website, the servers or whatever. The group of people to whom one has to pay particular attention are those who are vulnerable—minors, people with dementia and various other mental health issues, and disabilities. They often have little choice, but a huge number of people have access to their information, much of it being biometric information, and a number will have no training in what it means to behave ethically, to seek their consent and not to share data that should not be shared. That cluster has to be looked at as a special case.

Q26 David Tredinnick: Following on from what Stephen said—he has covered some of the supplementaries that I wanted to ask—it seems that one of the key issues is the human factor—the irresponsible user use of systems.

Professor Lodge, you talked about unanticipated use of biometric data. We could substitute, could we not, the irresponsible use of biometric data? Professor Amoore, you talked about internet online abuse. Is not part of the problem something that Stephen touched on? That is the tendency for people who are using e-mails to be trigger-happy. It has become a culture where it is such fun to press the button and forward something that is of no business to another person. It is a sort of chit-chat thing.

That goes back to what I was saying about using the post; you do not write an envelope and stick a stamp on it to send something unless you really mean to do it. Overall, if we are going to be successful in managing biometric data in e-mails and in stopping abuse, we need to have much more emphasis on human usage and teaching people how to do it.

Professor Black: It is about human education. We run a course with our students, and it is amazing when you go online exactly what you can find out about them; they are shocked that you can retrieve all that information about them. It is because they have almost a laissez-faire willingness to share everything and anything. There is a public education element as well. It is not just a nefarious use of information: it is a glib and laissez-faire approach.

Q27 David Tredinnick: Correct me if I am wrong, but I think the hackers who got into the celebrity websites looked at all the likely passwords that people would use—dates of birth, name of dog, name of street, all the simple things—which was clearly their downfall.

We went to the forensic labs when I had just joined the Committee. I remember poignantly our forensic experts saying how essential it is that people use obscure passwords. It is fundamental, but people are not doing it. A lot of this is just human nature, us being lazy. When we went into Libya, there were some special forces who were captured, and they had their passcodes for computers on them. That was absolutely against their training, and it caused all sorts of problems. I am not saying that they were ours, but it was a country's special forces.

Professor Black: It is about the fact that, on a day-to-day basis, we want to gain access and do not want to be inconvenienced. I can barely remember one password, let alone three, four or five. We become lazy and careless. It is a trade-off that the public often make to ensure that they gain access to do what they want to do. We know that we should not do it, but we all do.

Professor Amoore: It is for the convenience of the public, and it is also convenient in terms of governing various spaces. If you think about the smart cities agenda or the smart borders agenda, that is about trying to generate efficiencies by looking at various data sources and managing the flow of traffic or the flow of people using that data. The question of facilitation and convenience is part of this.

It is linked to how we live, and that is why these questions are so pressing. We live in a world where we want greater facilitation, and we want to be able to move. You mentioned terminal 2 and said what a great experience it was to move through that space, but in the background to your moving through terminal 2 were a series of automated algorithmic decisions about what sort of risk you posed as you moved through that space. Both of those things are involved.

Professor Lodge: One has to look at what you were saying about cyber intrusion. That is a big area of public ignorance. It exists on public misconceptions as to the balance between legitimate surveillance of some description and the kind of laissez-faire intrusion and laissez-faire approaches to privileged access, controls to one's own account and all kinds of other social media data that one may access.

Chair: Thank you very much for a very interesting start to our inquiry. We shall move on to our second panel. If the three of you are staying, I hope that there will be some seats available for you.

Examination of Witnesses

Witnesses: **Sir John Adye**, Chairman, Identity Assurance Systems, **Ben Fairhead**, Biometric Systems Engineer, 3M, and **Erik Bowman**, Systems Engineer, Northrop Grumman, gave evidence.

Q28 Chair: Welcome, gentlemen. It would be helpful if, for the record, you would introduce yourselves.

Sir John Adye: I am John Adye. I am chairman of Identity Assurance Systems, which is a very small start-up company. It is UK based but also with an offshoot in the United States.

Ben Fairhead: I am Ben Fairhead. I am a biometric systems engineer. I work for 3M in London.

Erik Bowman: I am Erik Bowman. I am from Northrop Grumman Corporation. I am from the United States. My current position is the chief engineer on the US Department of Defense Automated Biometric Identification System. My daily operations are to oversee the technical and engineering aspects of that biometric system, but I work, quite frequently, with our IDENT1 system, which is here in the UK from an engineering point of view.

Q29 Chair: Mr Fairhead, in your evidence you stated that, with the exception of face and fingerprint recognition, biometrics are unlikely to be in widespread use for many years to come. Can you explain why?

Ben Fairhead: What we were trying to say there is that you have the established biometric modalities of face and fingerprint, which have been used for many years. There are large existing databases of fingerprint and face, so there is an immediate benefit to using those in a biometric way. Other biometrics that are trying to compete with fingerprint and face have an uphill struggle to make their business case stand up. It is quite expensive to introduce a new biometric because you may need to introduce new infrastructure to capture that biometric information. If it is entirely new, there may be no legacy data that you can take advantage of to bring some benefit from that biometric, and biometrics are quite expensive to test. To really prove the accuracy of a new biometric modality, you need to test it with a large number of different people. It is like a drugs trial or something like that.

Q30 Chair: Do the other witnesses agree with that?

Erik Bowman: I completely agree. If I could expand on it a little bit, if you look at the world of biometrics, you can separate them from physiological versus behavioural. The physiological biometrics, including fingerprint, face, hand geometry, and so on, do not tend to change over time. They are well commercialised. On the behavioural side, you have voice and signature, which do tend to change quite frequently and give more frequent error rates. So I would agree with Ben in the fact that they are part of the commercialising, they are somewhat non-traditional, but they can be helpful as an additional biometric.

Sir John Adye: I see considerable potential in the development of iris recognition-based systems for this purpose, which can be done as the technology develops in a way which will be at the higher end of accuracy and reliability in matching purposes, and also in utility and ease of use, from some of the systems, for example, which are already in place for airport use in other countries, not so much yet in this country.

Q31 Chair: What are the commercial obstacles in developing new biometrics and how are barriers likely to be overcome in the longer term?

Sir John Adye: Maybe I could start on that because I am the tiddler here. These two are from very large organisations, both in this country and in the United States. The major part of the problem in this country, at any rate, is that we do not have the availability of established public trust, as was quite clear from the answers to your questions in the previous session. That is the primary inhibitor in this country, together with the fact that the present coalition Government cancelled, for good reasons, the identity card scheme. The new developments, which are being put in place, through the Cabinet Office's Identity Assurance Programme for public services, do not at this stage yet involve any use of biometrics. If we are going to rebuild or build anew public trust in this area, we must have good examples which get into public use for good reasons, with properly designed systems, so that people can understand how their data is being used and can start to use it through convenience and something which is useful to them.

Ben Fairhead: If I were to add anything to that, and if I understand the question correctly, you are talking about the commercial adoption of biometrics, maybe by the general public. We have seen that the banking industry has been quite slow to adopt the use of biometrics. It is dabbling in that area. In some countries—for example, in Japan—finger vein recognition is being used quite significantly to get cash out of a cash machine. Banks are wary because they are concerned about the ability to spoof a biometric—to use a fake finger, in other words, with a finger-print scanner or hold up somebody's face image to a facial recognition system. Until that side is sufficiently robust, the explosion of biometrics through remote authentication via a laptop or a mobile device is unlikely to take off, except for reasons of convenience and for low-value transactions, just like we use a contactless card for contactless payments for low-value transactions. We do not give a pin because, if somebody finds our card, the most damage they can do is £20.

Erik Bowman: I would agree with everything that has been said. I would add that most of the systems on which Northrop Grumman and the large integrators will work are mainly for force protection where accuracy is very, very important for that mission. A barrier, potentially, to advancing the engineering and the technology would be the availability to larger datasets than are available today in order to test. As was said by the previous panel, if you are going to build those biometric databases on which to test, whether it is with small or large companies, the consent to put in needs to be there as well. I would agree with the public concern that using biometrics is one of a communication issue.

Q32 Chair: Sir John, in your answer you commented on the ID card scheme and that it did not have the utility that people wanted out of it. People would be quite relaxed about carrying a card if it had some useful purpose to them. There is also the trust element and you referred to the previous witnesses. At the same time, even though the banks are being a bit slow, there is an extraordinary degree of trust. I suspect that almost everyone in this room has a piece of plastic on their person where they have given a huge amount of information to banks. Is that because the card companies and so on generate trust by saying to you, "Don't worry. If we screw up, we'll pay you back," or is there something more fundamental?

Sir John Adye: Chair, you have drawn attention to a very important point, which is that, in taking forward measures to increase public trust and use of good systems to identify people in the commercial or Government sphere, we need to build our developments on systems and procedures that demonstrably work. The payment card industry system, which you have just referred to, is an excellent example because it does work worldwide. You can go anywhere to draw money using your card, if you have the right credentials. It is instant and, as you have said, there is some recompense if somehow it is subverted. Much of that was developed and designed in this country with the introduction of the chip-and-pin system and so on. We need to build on that. We can build on it by adding, gradually, the use of biometrics. It need not be as an instant across-the-board provision of biometrics. It can come in gradually where they are obviously useful and as the technology develops.

Moreover, those systems, or systems based on a similar operational technology and procedures, can then be applied to other purposes using the same card or set of systems. For example, a case where we could make much greater use of biometrics already—it is scarcely done at all—is in health care services. I know my colleague on the left in 3M has several developments under way for the NHS and so on.

Ben Fairhead: Not in biometrics, I hasten to add.

Sir John Adye: Not yet in biometrics, but if you introduce them gradually in ways which actually work and can be explained clearly to the user what will be done with the data, you can do this provided you have an overall model for operation and an overarching framework, which was referred to by Professor Juliet Lodge in her evidence in the previous session. You need that kind of operational model to follow. It is successful with the credit card system, and you need the overall framework that is going to enable all of these systems to work together effectively in the circumstances of the internet. I believe that all of those things can be done if we approach them in an intelligent fashion.

Ben Fairhead: Just to add to what Sir John has said, we need to think about biometrics in terms of probabilities. We have already heard that from the previous session. If somebody takes your payment card now and they learn to forge your signature or they look over your shoulder at your pin number and make a transaction, how concerned is the bank about the risk of that? It happens all the time, but not enough that it is causing them a commercial concern. The same applies to biometrics. Yes, there may be a risk of somebody lifting my fingerprint from this bottle, manufacturing a fingerprint, stealing my phone or conducting an Apple Pay transaction in the US or something, but the effort involved for the damage it can cause is relatively limited. Biometrics is just another component in the whole identity assurance realm. Your location, the device you are holding, passwords, pins and biometrics can all be mixed together to varying degrees to give you a different level of assurance as to whether you know that person's identity or not.

Erik Bowman: You have touched on a very important point. Biometrics by themselves are not a panacea. When they are put into a security scheme for payments or things of that nature, especially in the consumer's eyes, it should be based on something you know, something you have and something you are. That, I think, is what he is touching on here, especially in the consumer realm.

Q33 David Tredinnick: Sir John, just going back to what you said—I am a member of the Health Committee as well—would you, please, write to the Chair of the Health Committee, Sarah Wollaston, about your views on biometrics for the health service?

Sir John Adye: I would be delighted to do so.

Q34 David Tredinnick: Thank you. Secondly, when you said that identity cards were cancelled for good reason, you went on to say that the Cabinet Office was not doing something, and I did not quite catch it. You said that they were doing some things but there was something you picked up that they were not doing. Can you tell us what that was, please?

Sir John Adye: Yes. I should make clear that it is not intended as, in any way, a criticism of what the Cabinet Office is doing.

David Tredinnick: Of course not. Just let us know what you think.

Sir John Adye: They have got to start with what is essential for putting in place an identity assurance programme for the delivery of public services in this country. They are making excellent progress with that relating to things like drivers' licences, tax records and whatever, which will be dealt with under the programme which is now in the initial stages of being rolled out. It was just an observation that, at this stage, none of the systems that I am aware of which are going to be provided under that programme use any form of biometrics. I may be wrong. There may be others of which I am unaware.

Q35 David Tredinnick: Thank you. It is just that you were the Director of the Government Communications Headquarters, so your views carry a lot of force, if I may say so. Could you tell the Committee if you think that biometric data is more valuable than other data that can be used to identify a person, please? Is biometric data inherently more valuable than other data that can be used to identify a person?

Sir John Adye: Yes, it is.

Q36 David Tredinnick: Would you explain why, please?

Sir John Adye: I believe that because, as came out from the three professors on your first panel, there is this absolute tie to the physical characteristics of the people. It depends on the form of biometrics, because biometrics can change over time in certain physical characteristics more than in others, but there is that absolute tie to the individual's inherent physical make-up or behavioural make-up. There is nothing that can easily be lost in that, such as a pin or a password. There is nothing that can very easily be faked by a criminal without the criminal being subject to the developing means of ensuring that the biometric credential is being submitted live at the time of transaction. For those reasons, I believe biometrics do add something.

Ben Fairhead: It is a deeply philosophical question because it depends what you mean by value.

Q37 David Tredinnick: I can help you there. Does it do the job better than other systems in terms of improving security? That is what we are trying to get at, is it not? It is not philosophical, I would say to you, with respect. It is about getting a result. We do not want to get lost in philosophy. Does it do a better job? It is a simple question. Is the system of biometrics more efficient than what has gone before?

Sir John Adye: May I point to another way in which it can do a better job? That is in enabling the anonymisation of data that is used at the point of transaction in an operational system. Systems of that kind can be used in ways which, through anonymisation, comply with the data protection regulations and laws in this country, the EU, the US or wherever it may be. For those purposes, you need to have, alongside the technology, the design of the way it is used. In some of the written evidence that this Committee has elicited, there is a particularly useful set of guidelines put in by the Information Commissioner's Office relating, among other things, to that process of anonymisation. Once anonymised properly, the data falls outside the provisions of the Data Protection Act.

Erik Bowman: If I can add to that, it depends on what the system is going to be doing. In a commercial system, where the system is being asked, "Are you who you claim to be?"—if that is the question that is being answered—then biometrics can be a little more absolute in terms of probabilistic matching than, perhaps, a pin, because you may, forgive the term, fat-finger the pin. I think the error rates for fat-fingering a pin are up around the 5% to 10% range, whereas biometrically it is 99% accurate.

Q38 David Tredinnick: Do you mean hitting the wrong digit or the wrong number?

Erik Bowman: Correct; yes. On the other hand, if the system is being asked the question, "Do I know who you are?", that is a far different question to answer. It is a one-to-many type of a search. You are trying to find a needle within a haystack. It is valuable because you are initiating the search based on a physical or behavioural characteristic, but the probability of that being matched among many, many images might be lower. Therefore, coming back to your original question of whether biometric data is more valuable, it is helpful if you are trying to find that needle within a haystack and you can aggregate data. However, when you are building a system that is doing a one-to-many or answering the question, "Do I know who you are?", you have to be careful on how you construct and secure the data so that it is not easily aggregatable by a person who has bad intent, because once you put that information together you have got that person absolutely. That is what you were touching on a little bit.

Ben Fairhead: Yes. Just to add to that, if you think of value in terms of security—you understand the concept of two and three-factor security—what you know, who you are and what you have, which are all ways of being able to identify yourself, whether biometrics is more secure than those other factors is very dependent on the specifics. It is an encrypted smart card versus something like a simple user name. There is a big difference.

Q39 David Tredinnick: Thank you. Mr Bowman, you told us that the security of biometric systems is all too often an afterthought. What steps need to be taken to ensure that security is considered from the outset when designing a biometric system?

Erik Bowman: That is a very good question. What needs to happen from the onset when you are thinking about putting in a system that is going to involve biometric and non-biometric data? It has been my experience that security is an afterthought because it is costly. In some cases, the agencies will not think all the way through a complete requirement that states you must protect the data in such a way, let the systems integrator figure out how to do that and then hold them accountable for protecting that data from the standpoint of having service level agreements or penalties levied against them if they don't meet those requirements. It has been an unfortunate afterthought, but, as biometrics become more prevalent within systems, the security will be thought about, architectured and implemented up front before the system goes live. It has been my experience that it just has not. It needs to be done from the outset.

Q40 David Tredinnick: Google has been in the news in the last couple of days with the problems relating to the murder of soldiers and whether the security services had the right information. Do you think that search engine organisations should have penalties? I think that was the word used. Do you think that there should be much stronger sanctions against those who manage data systems to encourage them to be more security-conscious?

Erik Bowman: When you put in systems that are going to have data such as the ones you are mentioning, security is of paramount importance given the value, as you pointed out earlier, of the data inside that system. If security is breached in any sort of way, they should be held accountable for the requirements they did not meet. That is why I would rather see those stringent requirements up front so that everybody knows what they are getting into prior to bringing the system forward.

Ben Fairhead: From my experience in the UK, security, certainly on the Government side, is very well thought about during the whole procurement stage and it is designed in from the outset. That has certainly been my experience.

Q41 David Tredinnick: Thank you. Finally, what mechanisms are already in place or being developed to protect stored biometric templates?

Erik Bowman: When the data are at rest, meaning not being used or in the process of being authenticated, they can be encrypted. The template itself is a small representation of the image itself. It is fairly hard to reconstruct into the actual image. The images are kept separate along with the security scheme and can be encrypted, but that comes at a particular price from system performance. So it is a trade-off depending on what the system needs to do. You need to trade off the security with the performance aspect of it.

Sir John Adye: If I might add to that, with which I fully agree, the new development that we have to take account of here, which is actually a very positive one, is the beginnings of the availability of the use of biometric sensors on mobile phones, on mobile devices, where the notable factor is that the use of biometrics is unsupervised by the relying party in this case. If you go to an ATM to put in your credit or debit card, that system is going to be supervised by the bank in some way, but when you are using your smartphone, or even your PC at home, there is no physical supervision of the system. So you need to design security methods to apply to that mobile use that are going to be strong to protect the

interests both of the individual who is using the phone and the relying party at the other end, which is the bank or whoever it is, which is providing some service to them.

Q42 David Tredinnick: Forgive me for interrupting, but are you saying that the mobile phone companies are not using biometric data systems properly at the moment in that they are not secure?

Sir John Adye: No. They have made a good start.

Q43 David Tredinnick: But you are not happy about it.

Sir John Adye: No, I am not happy. It needs to be developed further. The main problem is that there is no public visibility of what measures they have put in place. For example, you just cannot get at what Apple is doing on the iPhone 6, where they have introduced it. You can only infer from the way they are doing it what the security procedures are. We must find ways of corralling these big giants of the internet so that they work properly.

David Tredinnick: Thank you. I have just realised that I have strayed into my colleague's question. Forgive me for that.

Q44 Pamela Nash: Can I just clarify the explanation that you just gave about your concerns about the security of using biometrics in mobile devices? Is that what you meant in the written evidence of your company, which stated that it was "technically challenging to implement" biometrics remotely? Was that your full concern or is it that the miniaturisation of that technology is not yet of high enough quality to cope with those risks?

Sir John Adye: The technology does need to be developed further in some respects, but the primary problem is this one that I referred to earlier—that the smartphones, or whatever, are outside the control of the relying party, and, in consequence, it is necessary to have the right kind of security and cryptographic techniques designed into the systems which are on the phones themselves and then the systems which use the information transmitted from the phones to make some kind of a match of credentials—not necessarily biometrics; it can be other credentials as well—in giving access to the individual, let's say, to their bank account. So it has to be designed as a whole system all the way through. The same principles need to be used for all such systems so that public trust can be developed in them. So far, that is not the case. At the moment, all this area of use on the internet is a jungle. I don't know, although I am quite experienced in this field, what happens to my personal data when I use them on a smartphone for proving my identity. Is Google going to use that data also to target advertising at me? Is some other commercial company or maybe some hostile foreign Government going to use it to target me in some other way? I don't know. We need to find ways of getting that kind of system properly organised.

Q45 Pamela Nash: Is that a problem that you think can be tackled just by the technology used and transparency, or is that more a question of regulation?

Sir John Adye: No. It does need to be tackled through the development of the technology but, more importantly, the design of the systems which use the technology. You cannot do it by regulation, or at least it is extremely difficult to do it by regulation, because the internet is not the province of any one Government. In consequence, all the Governments around the world are looking at this for various purposes. The only way you can take it forward is by developing international standards which it is in the interests of the companies that develop these systems to use, and demonstrably use, so that they can assure their customers that they are properly protected. Unfortunately, it is a slow process. We do not yet, for example, have international standards for the use of biometrics on mobile phones and any devices outside the control of the relying party. Those standards are in the process of being developed, but, because they have to be agreed across all the countries concerned, it takes time. In the meantime, companies like Google and Apple are introducing procedures that people are going to be using. We cannot regulate them; so we have to make it in their commercial interest to have the right kind of systems in place so that they make more money out of doing it in a safe way, which is useful for the people who use their services.

Q46 Pamela Nash: You mean basically putting people off from using those services if they are not secure—that there is a commercial interest in that.

Sir John Adye: We can use all sorts of public forums, like this one, to educate people on the subject, to encourage them to ask questions and to think twice before they tick that box. If, for example, they are using the Apple iPhone 6 to use it for Apple payments, which has just been introduced, you can now use your iPhone 6 to make payments, using biometrics, on the internet. You have got to tick various boxes before you do so, but how many people are actually going to read through all of those boxes properly and understand what they mean when it goes in?

Chair: Read the report that we are just about to publish.

Q47 Pamela Nash: Sir John, just before I ask your colleagues what their views are on this matter, do you have any reason to be particularly concerned about the technology used by Apple at the moment, or is your concern based mainly on the fact that there is no transparency in the technology?

Sir John Adye: Apple has, clearly, done some good things in what they have designed. They appear to have a good system at the moment for protecting their operating system so that it is difficult for anyone from outside to penetrate it and retrieve data from it. How long will that last, because criminals and other people are very inventive in finding ways in? Secondly, although you can protect it in that way on the device itself, what happens if the device is lost or stolen? In my view, you should always delete from the device any evidence of the credentials used for a transaction immediately after the transaction has taken place. That does not happen at present and I think it should.

Q48 Pamela Nash: Do you mean that that would be automated?

Sir John Adye: Yes.

Ben Fairhead: I do not have much to add, but just to emphasise, as Sir John was saying, the need for open standards. There is the Fast IDentity Online alliance initiative to develop standards around client authentication in biometrics. In the case of Apple, they do have some kind of security module in the phone that acts like a smart card or a phone card effectively. That is where the biometric data is stored. I guess it is similar to losing a bank card. If you lost your bank card and there happened to be a copy of your fingerprint on it, or a passport even—in Germany, people have two fingerprint images on their passport held in a chip—if they are lost, it is fairly unlikely that an attacker would be able to release those due to all the cryptographic mechanisms in place, but, as Sir John states, we do not really know the details with respect to Apple.

Q49 Pamela Nash: You referred earlier to the risks that would be involved in using biometrics in a remote location. I was quite shocked when you said that some facial recognition systems could be fooled by a photograph. Is there anything else that we should be aware of? Can I ask what your company is doing to try and tackle this risk?

Ben Fairhead: There is a whole science around liveness detection, anti-spoofing and all sorts of methods that you can employ to try and work out, "Is this finger made from rubber?" "Is it made of flesh?" was the question you were asking, and, "Is there blood pumping round it?" So is it a spoof and is it alive? There are multiple techniques, and they have matured quite a bit, certainly since I have been in the industry, but they still introduce other issues. Basically, you get spurious results. If you are an unfortunate person who has got, say, Raynauld's syndrome or you haven't got much blood flow through your fingers, it may be that the system does not think that your finger is alive when you are presenting it. You have got those kinds of issues to deal with. It still ends up being an arms race between you and the attackers—or an arms, legs and fingers race. For example, if you check the conductivity of a latex finger, the attacker will put iron filings in to match the conductivity of human skin. Now we have got to come up with some new technique to prevent the fakes. One of the best techniques is using multiple biometrics. So we are seeing a demand for multi-modal systems which use face and fingerprints in the same system, because it is a lot harder for somebody to manufacture finger or several fake fingers, a facial image and irises, or whatever, all in combination.

Erik Bowman: What Ben is touching on is, again, back to the security scheme. If you are going to be using a biometric device in a remote location, such as an iPhone or something of that nature, or an android phone, don't rely on just one security factor. Rely on multiple, whether it is multiple biometrics or if it is multiple authentication schemes, be it a pin, a password, a digital certificate and a biometric, and then, obviously, something you have, which is the phone itself. It becomes harder to spoof when you are relying on multiple authentication schemes within an overall security architecture.

Sir John Adye: That, in fact, is already incorporated. I said earlier that the biometric standards for this purpose have not yet been fully developed, but there is an excellent set of standards on overall security procedures already in place through the ISO, which demand what Erik has just put forward should be done for higher levels of assurance—that you have to have multi-factor authentication in those cases.

Q50 Stephen Metcalfe: A lot of what I wanted to cover has already been explored. There was some sort of universal acceptance around developing open standards for biometrics. Concerns have been raised that large technology manufacturers are using proprietary standards. What role do you think the Government have, if they are not going to legislate, in encouraging open standards, or businesses and organisations to comply with open standards?

Ben Fairhead: As a large supplier of biometric technology—it sounds like a plug—we are standards compliant, as our systems have to be because Governments demand that the sorts of systems we supply are standards compliant. The systems we supply need to talk to other systems within a country, and sometimes between countries, so they have to comply with certain data standards otherwise they could not exchange information. Biometric standards are very widely adopted today. Historically, there has been quite a lot of use of proprietary standards. Part of the reason for that is that the international standards were not really mature at that stage, when you were sending data over a slow telephone line, if you wanted a very small bit of information sent over. We do not have that problem any more. We can send images that anyone can read, potentially, although obviously encrypted.

Q51 Stephen Metcalfe: So things are improving, in your view.

Ben Fairhead: Yes.

Erik Bowman: What Ben touched on was data transmission and standards for data transmission among fingerprint images, faces, irises, and, to a certain degree, voices are fairly well established on the international scale, so that systems can accept the raw image and do something with it. I have seen attempts in the United States to create a common template that the Government would own and license out. That was not successful because Ben and his company are in the business of creating fine, good intellectual property that can find the bad people, so to speak, or can find the needles in a haystack. We, as a systems integrator, take the algorithms that they do and put them into a system, or they put them into their own systems. So walking a fine line between intellectual property as well as trying to have a common template that would be working across all vendors is very difficult.

Sir John Adye: I entirely agree with what my colleagues have said. There is an additional point as to what can be done to encourage good practice or in regulating. I said earlier that you can't regulate what happens on the internet, but you can regulate what systems employed in particular countries are required to do by the law. We have already referred to the Data Protection Act and so on in this country, which implements the EU legislation in this matter. There is a lot of debate at the moment, particularly in the European Community and sponsored by the European Commission, into ways in which that law and those regulations should develop. It will be necessary, then, for any system which is deployed in any of the countries of the EU, at any rate, to comply eventually with that regulation on privacy, security and so on. I am concerned that the UK is, perhaps, not proactive enough in influencing those developments in the European forum and putting forward UK views on how it should be done. In my written evidence, I have drawn attention to some of the particular areas where that is proceeding. I would hope that, maybe, we will do rather more in that field.

Chair: Gentlemen, thank you very much for your evidence this morning. It was very helpful. We will go straight on with our third panel.

Examination of Witnesses

Witnesses: **Andrew Tyrer**, Head of Enabling Technology, Innovate UK, **Emma Carr**, Director, Big Brother Watch, and **Dr Peter Waggett**, Chairman, British Standards Institution technical committee IST/44, gave evidence.

Q52 Chair: Thank you for coming this morning. Again, it would be helpful if you could introduce yourselves.

Andrew Tyrer: I am Andrew Tyrer from Innovate UK.

Dr Waggett: I am Peter Waggett. I work for IBM but I am here as the chair of the British Standards Institution's Biometric Standards Committee.

Emma Carr: I am Emma Carr. I am the director of Big Brother Watch.

Q53 Chair: According to the Government, biometric identification systems should demonstrate "a lawful purpose, a pressing need and proportionality". Are these principles reasonable and do current systems observe them?

Andrew Tyrer: In terms of proportionality, the majority of businesses that we deal with and have invested in have that in mind. A lot of the calls and the innovation work we do in the area insist upon that and we make sure that people have the right processes in place while they do that. The challenge is that a lot of small companies and start-ups, if you think of people in Shoreditch and Tech City, are starting to build systems very quickly. Digital systems can be built over a weekend, effectively. Do they take into account the necessary controls and have procedures in place when those organisations might not, for instance, be a security company?

Q54 Chair: Maintaining proportionality is incredibly difficult to achieve in practice.

Andrew Tyrer: In that landscape, yes.

Dr Waggett: One of the things that we have been doing at the BSI has been developing a code of practice for the implementation of biometric systems, and that is really a 101, if you like, in how to develop a biometric system that fits into those criteria. It has specifically been targeted at small to medium-size businesses so that they can pick up and make sure that they are adhering to those restrictions.

Emma Carr: I agree with all of that. Building privacy and necessity into whatever system you are designing from the outset is incredibly important. From Big Brother Watch's own research into this area, we were very interested to look into the use of biometrics in schools. I would direct you to our report called "Biometrics in Schools", which we published last year, and it showed that 40% of schools at present have biometric systems in place, whether that be for cashless catering, library books or registration. In our view,

from taking a look at that, a lot of the time it was because it was new and they thought it would be the most technologically advanced thing to have in their school. A lot of new-build schools had this sort of technology, and they could not give a direct reason as to why it was necessary for them to have it rather than another system.

Q55 Chair: What changes do you think are necessary to make sure that the principles the Government set out are adhered to?

Emma Carr: As I say, having a clear plan as to why you need that system in the first place, looking at the principles and thinking about privacy-impact assessments and things like that, is a very good starting point. I know that, in terms of simple guidance in this area, within the public sector, it is largely adhered to. As we have talked about in regard to the private sector, there is an arms race, so to speak, in wanting to be the next people to design the newest piece of technology or the newest way to use biometric systems. So, potentially, guidance is not as adhered to as you would see in the public sector.

Dr Waggett: Again, I come back to this practice we have developed. We have had success with that, to the extent that we are now taking it forward as the basis of an international standard.

Q56 Chair: That is what I was going to ask you immediately. From the earlier evidence sessions, it is pretty obvious that we need international standards. There have been examples in the IT sector in the past where BSI has been in conflict with other international players—for example, the development of open standards for XML. It took a long time to establish those standards. Major players, such as the British Library, were really anxious about the delays they were caught up in. Are we confident that there is enough drive inside the international arena to get the kind of progress that both Governments and society want to see?

Dr Waggett: From experience in attending the ISO meetings and helping to develop and editing a couple of the standards, I would say yes. We have found that there have been waves of standardisation. First of all, it has been set up for the large-scale systems that have been used for airport border control and things like that. We are now looking at a new raft of standards that are coming out, particularly around mobile consumer devices, around new technologies that are going to be coming through and new modalities. There is a rolling programme of doing this. It is not easy because we have to gain acceptance and buy-in from all of the different nations that are represented at the ISO level.

Q57 David Tredinnick: Ms Carr, your Big Brother Watch raised concerns about technologies that can collect biometric data covertly and use it to identify people without their knowledge. Are these technologies, in your view, widespread in their use and, if so, who is using them?

Emma Carr: It is hard to tell whether it is widespread because it is covertly.

David Tredinnick: It is like "The Secret Policeman's Ball".

Emma Carr: In terms of the research that we are conducting—we are not specifically looking at biometrics; we look at many things—one of the things that really jumped out to

me when we were putting our written consultation together was the story about the NSA collecting facial recognition photos from the net. They said that they will not access these photographs for identifiable purposes, but they do not have access to the databases of photos for things like passports and drivers' licences. So, instead, they were reverting to going through people's online posts, video messaging and that sort of thing to try and get the images in that way.

Clearly, consent is a huge issue there. As much as I would not advocate them necessarily having direct access to our photos via the passport and driving licence database, at least, if that was the case, you could go through a system of informing the public that it would then be used in that way and go through a consent process of informing the public. However, if it is essentially trawling through the net to see what we have posted on it, it is probably not as accurate; after all, if you look at anybody's Facebook page, for instance, they may look very different in lots of different photos, depending on what they are for. So accuracy is a huge problem, but, indeed, for us, consent is the biggest issue here.

Q58 David Tredinnick: Dr Waggett, you have previously said that stopping people being observed via biometric systems is not going to be feasible. Can we control how that biometric data is collected and subsequently used or not?

Dr Waggett: Yes. A lot of focus has been, effectively, on trying to prevent images being taken. What I was trying to get across was that that is not really an option because of the proliferation of cameras all around the place. Every smartphone now has two or three cameras in it and it has a video capability. There is a lot of imagery being collected of individuals. The bulk of it is not by Governments. It is by organisations and/or peers, just people passing it around. We need to focus on providing the other aspect of privacy, which is not being disturbed by that observation, and providing technologies that can help with that. For me, that is a big issue in how we ensure that people are not impacted, even though they may be just under general surveillance through cameras that happen to be in place.

Q59 David Tredinnick: This is a question to all of you. Do you think that the current legislation adequately addresses the challenges that these covert techniques present to privacy and control over personal data?

Andrew Tyrer: I think the legislation for Government use is adequate. The challenge is legislation for private use when you are not given that privacy and consent. In other words, if a commercial organisation is taking a video of you in a street and you have not consented to give that information, they use that information and it becomes personal information, then you have not consented to use that. From a Government perspective, of course, I am sure that Government agencies would act according to the regulation. Therefore, I do not think it would be a challenge in Government, but certainly out in the private industry it can be a challenge. You would not even know it was going on, to be quite frank, so that could be a problem.

Emma Carr: There is a huge need to strengthen the potential punishments for people who maliciously abuse access to our information. Big Brother Watch has called a number of times for custodial sentences and criminal records to be introduced for the most serious of

data breaches. I believe it would be a relatively easy thing to do. What we do not want to end up doing, especially for private companies, is for them to see these relatively small fines as a cost of doing business. We need to avoid that at all costs.

Q60 David Tredinnick: Are you saying that the sanctions should be personal rather than corporate?

Emma Carr: Yes, in some cases.

Q61 David Tredinnick: Directors should personally be liable rather than companies.

Emma Carr: Or, indeed, the individual. We have seen, especially within NHS cases and medical record cases, individuals who have ended up maliciously accessing people's medical records receiving a relatively small fine; so there is nothing really stopping them from doing a similar job elsewhere, having similar access to people's records. That is something that needs to be addressed.

Q62 Chair: Have you not just created a slightly circular argument here? You heard what Sir John said in his evidence earlier on. You have just said yourself that the NSA is capturing data. Mr Tyrer responded by saying that this Government are doing things in a regulatory sense correctly. Because of the whole nature of the web, as Sir John explained, we cannot impose regulations upon other Governments and companies outside the jurisdiction. How are you going to make it work in practice?

Dr Waggett: If I can follow up on the original question, we need to make sure, where somebody's privacy has been impacted and they have suffered loss from that, that the punishment ought to fit the crime that has gone forward. We may not be able to legislate about people's data being taken, but, surely, if somebody has had some personal impact from that, then that should be remedied.

Andrew Tyrer: I think that the change is one of scale, where the Government should know what the regulation is and abide by it, as should big businesses. Small companies should, but their lack of awareness is a problem. Small companies do not realise. It is not malicious activity. It is just activity about which they do not realise they are maybe breaking laws and regulations. Some activity needs to be undertaken where these new technologies are used so that people know their responsibilities. That goes for all data protection, not just biometrics.

Emma Carr: I agree. If you look at the updating of the EU Data Protection Act as well, that is a step towards international norms and standards of what is expected not only of Governments but of businesses as well that operate in a certain sphere. That is always helpful.

Dr Waggett: As an educational view, the code of practice is something we should keep pushing.

Q63 Chair: I still struggle. If I am operating in a foreign jurisdiction outside the EU, I capture your data off a site and I use it for some other purpose, what is the jurisdiction that is going to prosecute me? There is not some international court that is going to be doing this.

Emma Carr: I am not an expert in what the new data protection legislation is looking like, but I believe there are parts in it about what information should and can leave the EU and how it should be dealt with. I think they are starting to attempt to address that, but whether that is sufficient or not somebody else would need to answer.

Q64 Stephen Mosley: Both of the previous questions moved on to the question of standards, and I was going to ask about standards. There are standards out there. Do you think that those standards are currently being adhered to?

Dr Waggett: Yes, very much so. In my day job with IBM, I have been developing biometric systems for about 20 years. In those instances, we are already using the ISO standards as we go forward.

Q65 Stephen Mosley: What about outside IBM and in the wider world? Are they using them?

Dr Waggett: We have quite a big pick-up in the usage of standards across the globe. Our remit is to get standards to a point where they can be accepted as an international standard and then all the different nations buy into those. In particular, if the Government are procuring a system and are using those standard sets, then they know that they have a number of potential vendors who can deliver to those standards.

Q66 Stephen Mosley: In response to the Chair, you said it was difficult drawing up these international standards. How do you balance the differences between industry and Government and the differing needs that they both have?

Dr Waggett: The British Standards Institution is very good at gathering a large number of stakeholders. I am there as an industry representative. We have academics and consumer groups represented as well. That broad church enables us to put forward a coherent set of views. It is done by consensus so we do have to negotiate, but we have had very good representation at ISO meetings that has enabled us to get to a point of view that makes sense both for Britain and also the industry.

Q67 Stephen Mosley: What are the incentives for commercial organisations to adopt the standards?

Dr Waggett: If we look at what we did for the UK Border Agency system, we put forward what was, effectively, technically called a service warranted architecture. That allowed us to limit the biometrics to a simple biometrics-matching service, and to go to a range of different vendors and come up with a solution that would fit and could also move forward in time. The good thing for that in terms of the vendors is that it enables them to concentrate on building the better mouse trap, if you like, the better matching service,

while not worrying about system aspects that are handled by the integrator as part of their activities.

Q68 Stephen Mosley: Looking at privacy, which we keep coming back to, are there any risks or advantages for personal privacy on having widespread use of standards?

Dr Waggett: I am not aware of anything that would come through from that point of view in that all of the datasets that we have can be encrypted. They can be encrypted independently so we can protect privacy at source. We can also use technology such as cancellable biometrics, which is where you take the biometric, contort it in a known fashion and then match it in a contorted space. The advantage of that is that the data is never stored anywhere in an unencrypted form. You match in that form, which means, for example, that if a biometric is leaked out and somebody has found that out, you can change the distortion and recreate the system.

Q69 Jim Dowd: I come briefly to a question of public trust in biometrics. Dr Waggett, you stated that the rapid pace of development in biometrics can mean that "consumer concerns are not recognised until it is too late". What action needs to be taken to ensure that public concerns are both identified and addressed earlier?

Dr Waggett: From my perspective, we are looking to strengthen our input from other consumer groups to make sure that we represent those at the international level. There, clearly, is a line in terms of when something becomes an issue as to when we can address it. I am very thankful to my committee because they are working as hard as they can to make sure that we push these things and that the consumers are protected.

Q70 Jim Dowd: Does anybody else want to say anything?

Andrew Tyrer: The challenge is also about adoption. There is consumer protection, but, quite often, if you look at a lot of systems on the market, their design is from a technical point of view and not a user point of view. The concern is that people do not understand how to use these systems appropriately. Therefore, not only are they quite often fearful of them, but allowing a system to become complicated allows them to be spoofed and weaknesses can be injected because people do not understand how to use them appropriately at the time. Therefore, people can inject errors maliciously, potentially, into the system if they want to. There is a challenge around some consistency about the design implementation of products as they emerge in the marketplace.

Q71 Jim Dowd: On that point, is it possible to make the development and implementation of biometric systems more transparent to the public and, if so, how?

Andrew Tyrer: The challenge is around the intellectual property within people's algorithms and systems. There is a challenge there. There is a gap in the market, as previously was discussed earlier, around the testing of systems, how interoperable they are and how they sit alongside their peers. A lot of the rigour that goes into testing is quite often fronted by the manufacturers themselves. Therefore, there is not a lot of independent

activity. There is some that goes on in the United Kingdom. For instance, the National Physical Laboratory does independent testing, as does NIST in the United States. I sit on the Cross Government Biometrics Working Group. In that working group, other Government Departments also talk about the systems they might use and how you might test those. So a lot of thought has come from a Government perspective. Out in industry, there is a challenge around whether it is a cost element or a design element. People might not think immediately around how they design in terms of not only a user interface but security as well when using those products.

Q72 Jim Dowd: Finally, should there be an alternative to enrolling in biometric systems and should that choice always be available?

Dr Waggett: One of the things that we have to be aware of is that we cannot have a digital divide. We cannot have our systems that are set up that only have the biometric involved in them. Some people may not wish to participate in that, but, clearly, what we cannot do is to have a system from which they cannot get the benefits. There must always be alternatives, if for no other reason, let's say, that somebody may not have reasonable fingerprints to capture. My father suffered from cancer, and as part of his chemotherapy the drugs that he was given removed all of his fingerprints. Actually, he was in a situation that he could never give a satisfactory set of fingerprints. He must not be excluded from getting the benefits from any kind of system.

Andrew Tyrer: You only have to look at the announcement by the banks a few years ago that they were going to stop cheques and the confusion and panic that that caused in various sectors, but also with people who might be digitally excluded. It would be no different from that. If you look, for instance, at car tax, the majority of us who are happy online do our car tax online, which is easier, but you still need the default of a post office to go and do it if you are excluded in that way. I do not think that biometrics will be any different.

Q73 Jim Dowd: The banks were, of course, forced to relent from that position.

Andrew Tyrer: Indeed, yes.

Emma Carr: If you look at the Protection of Freedoms Act and the use of biometrics in schools, it says that children and parents have to have a second option if they do not want to use biometrics. That is quite a radical piece of legislation. If people are unaware, it says that you have to have written consent from a parent or guardian, but you also have to seek oral consent from a child, and, if the child says no, the child's oral consent can override a parent's written yes. That is a hugely important step in starting to educate young people about why we are being asked to hand this over, what is going to be used, how is it going to be used and who is going to have access to it. It is a matter of starting to get them to think about those really integral questions which will set them up for later life.

That brings me on to something about which we have been getting a lot of letters and e-mails, which is something called Clubscan. It is now the norm in a lot of clubs in the United Kingdom that you have to hand over your driver's licence or passport, which is scanned, when you first enter that club. That happened to me recently, and then when I

wanted to put my coat in the cloakroom they said that the only way I could do that was by giving my fingerprint. I said that mine will be the one without the fingerprint. I am thinking about how people can give full consent if it is 2 o'clock in the morning if you are asked to hand over your driver's licence, as a usual form of ID and, before you know it, it is being scanned. In trying to find out who has had access to it, how it is deleted and whether they know what their obligations are under the Data Protection Act, is it actually proportionate under the Data Protection Act to use that for a cloakroom and not be given an alternative option? A lot of these companies just do not understand what it is that they have sold themselves into.

Q74 Chair: I shall not delve into the nature of the clubs. Dr Waggett, you were once a member of the Biometrics Assurance Group.

Dr Waggett: That is correct.

Q75 Chair: What has happened to that?

Dr Waggett: Because of the fact that my company was bidding for work that was going on, first, with the UK ID card scheme and then, secondly, the biometric waiver scheme, I had to remove myself from it.

Q76 Chair: Is the group still in existence?

Dr Waggett: I do not believe it is. Certainly a lot of the members are active within Government. The Home Office has a very strong biometrics lead and also it has a group that is providing advice.

Q77 Chair: Mr Tyrer, you are a member of the Government's Biometrics Working Group.

Andrew Tyrer: That is correct; yes.

Q78 Chair: Tell us about that group and what is its current status?

Andrew Tyrer: Basically, the group is championed by the Home Office and, in particular, CAST, which is the Centre for Applied Science and Technology—the old HOSDB. Basically, it has interested members from Government who talk in a very informal format around the challenges of biometrics; it meets quarterly and it gets in speakers from industry. Every agenda has a focus, so it might be around standards or it might be around facial recognition; so it has a focus. Then we will try and bring in organisations that are active so they can understand across Government what is going on and what the challenges are that Government Departments might have.

Q79 Chair: Is it established as a scientific advisory group?

Andrew Tyrer: No.

Q80 Chair: What status does it have, do you know?

Andrew Tyrer: It does not have a status. It is an informally connected group that meets on a quarterly basis. I don't think it has any status as a Government body as such.

Q81 Chair: It seems to me that there is a missing bit there, isn't there?

Andrew Tyrer: Potentially. You would have to speak to the secretariat.

Chair: Thank you very much for an informative session. That concludes our session this morning.