HOUSE OF LORDS

Justice and Home Affairs Committee

Corrected oral evidence: New technologies and the application of the law

Tuesday 22 June 2021

10.30 am

Watch the meeting

Members present: Baroness Hamwee (The Chair); Baroness Chakrabarti; Lord Dholakia; Baroness Hallett; Lord Hunt of Wirral; Baroness Kennedy of The Shaws; Baroness Pidding; Baroness Primarolo; Lord Ricketts; Baroness Sanderson of Welton; Baroness Shackleton of Belgravia.

Evidence Session No. 1 Virtual Proceeding Questions 1 - 24

Witnesses

I: Professor Sylvie Delacroix, Professor in Law and Ethics at University of Birmingham; Professor Charles Raab, Professor Fellow, Politics and International Relations, University of Edinburgh; Professor Carole McCartney, Professor of Law and Criminal Justice, Northumbria University.

USE OF THE TRANSCRIPT

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

Examination of witnesses

Professor Sylvie Delacroix, Professor Charles Raab and Professor Carole McCartney.

Q1 **The Chair:** Good morning and welcome to the House of Lords Justice and Home Affairs Committee, the first meeting where we are taking evidence on new technologies for law enforcement.

I have some housekeeping points to start with. The session is being broadcast and a transcript will be taken, which our witnesses will have an opportunity to review before it is published. I will bring in members to ask questions, but, if people want to come in, there is the hand-raising function, as distinct from the physical function. We have an hour and a half or so for this session. We will give about five minutes to each question, and there will be time for supplementaries at the end. I ask members and witnesses to remain muted when they are not speaking, and I remind members to declare interests when they first speak, as this is the first evidence session.

I warmly welcome our witnesses to the first evidence session on new technologies for law enforcement across all its aspects, and I will ask them to introduce themselves in a moment. We are now scoping that inquiry, and your evidence will help us to identify what we need to explore in more detail. Can I ask you very briefly, in alphabetical order, to introduce yourselves?

Professor Sylvie Delacroix: Thank you for inviting me today. I am professor in law and ethics at the University of Birmingham, a fellow at the Alan Turing Institute, and a Mozilla fellow. I have worked on various issues involving algorithms in the justice system, particularly as a commissioner for the Law Society of England and Wales report two years ago.

Professor Carole McCartney: Thank you. I am pleased to be here this morning. I am professor of law and criminal justice at Northumbria Law School at Northumbria University, where I also convene a research interest group in science and justice. For the last 20 or 30 years, I have been researching primarily in the field of forensic science but now biometrics and other technologies within the criminal justice system.

Professor Charles Raab: Thank you and good morning. I am a Professorial Fellow at the University of Edinburgh, where I was Professor of Government. I am a fellow of the Alan Turing Institute and I co-chair the Data Ethics Group there. I am also a member of the Home Office Biometrics and Forensics Ethics Group, although I am here in a personal capacity. My research over many years has been in the area of privacy, data protection, surveillance, the regulation of information technologies, and things in that general area.

Q2 **The Chair:** Thank you. First, I have a very general question. As I have said, the session is looking at new technologies being used in law enforcement settings. Can you each tell us in turn what you are seeing being used, how widely and in what settings? I appreciate that it will be difficult to do all that in five minutes in total

and, if necessary, a couple more minutes. Professor Delacroix, let us start with you.

Professor Sylvie Delacroix: I can speak about what we gathered as evidence during the commission hearings two years ago for the Law Society. One of the things that was striking is that these predictive tools have entered public awareness fairly recently, mainly due to reports based on US use. In the UK, these systems have been in use for some time. Initially, I think they were used for predicting burglaries, and that was in 2004 or 2005. Since then, there have been other systems. I am not a specialist like my two colleagues here in particular technical interventions, but I am struck by the extent to which there have been many local initiatives but so far, I think, a lack of national debate on this front. That is why I think this committee's work is so important.

Professor Carole McCartney: I endorse what Professor Delacroix said, although I doubt that I have any more clue or precision about what is going on. That would probably bring us to my first point—if there was any that I would like to make—about transparency and accountability. I am not sure who you could get in front of you who could answer that question with any kind of comprehensiveness.

I know of snippets. Obviously, I know of the forensic developments that are being used, and biometrics and how they are used. We have all heard now, because of controversies, about automatic facial recognition. We have heard about the Gangs Matrix, databases and so forth. Of course, some of these technologies have been in place locally for some time, but I do not know who you could ask who could actually give you a decent, comprehensive answer to that question.

Research has been done. Babuta and Oswald did a survey. We know there are things going on. We hear from the West Midlands Police, which has an ethics board that reviews things, of potential things coming up. We have also started hearing about polygraphs being used increasingly. But, like I say, my answer is that I cannot answer.

The Chair: Thank you. That is why we have started this inquiry.

Professor Charles Raab: I hope that we can return to the issues of accountability and transparency, but on top of what has just been said there are a whole range of uses of new technologies, or experiments in using them, or discussions about them, including things like voice recognition, gait recognition and the detection of emotions or sentiment, which might feed into some algorithm to analyse people's disposition to commit crimes or whatever.

There is a greater use of live facial recognition technologies, which has received an awful lot of publicity as well as criticism; the use of drones, which have cameras in them and are used for crowd control and so forth; the searching of mobile phones; the searching of databases; and a whole range of other things for crime mapping and for individual targeting.

As Professor McCartney said, there are a lot of technologies and applications out there at different stages of development, deployment or non-deployment, but it is very hard to get a comprehensive, deep answer to many of them.

The Chair: Indeed. As I said, we want to know and the public want to know, and we would like to find out how much government and its agencies actually know.

Q3 **Lord Ricketts:** I think that what our witnesses have already said shows how important this inquiry could be. I would like first to declare two interests. I am a strategic adviser to Lockheed Martin UK, and I am trustee and soon to be vice-chairman of the Royal United Services Institute.

I want to pursue a bit further the opening question from Baroness Hamwee about what is actually going on. We are learning that law enforcement is increasingly using a range of these data analytic tools and algorithms to make judgments that perhaps previously were made by human beings. We have heard not only of facial recognition but of the use of these tools to predict the risk of reoffending and of committing domestic violence, for example.

My colleagues will come on to the legal, ethical and accountability issues, but I wanted to probe a bit further on a basic layman's question. Do these technologies actually work? Do they deliver what they are designed to deliver? Are they designed with sufficient rigour so that they produce the outputs that they are being used for? I know that it is a rather general question, but it is to get a sense of how you see that. You are a lot more expert than we are, even if you are not scientific and technological experts.

Professor Sylvie Delacroix: This is an important question. What strikes me is the importance of not answering that question in general. When you ask whether these tools work, you have to have a very clear and agreed definition of what exactly these predictive policing tools are trying to predict. If it is burglaries, it may not be too problematic, but if the idea is that they should predict future crime with no further specification, they definitely will not work. Why? They are not meant to work in that way, in that we do not know who has committed crimes in the past, since most crimes are never reported and some crimes are reported falsely.

Instead, often we use arrest as a proxy for crime because we know who gets arrested, but the problem is that even the best law enforcement agencies do not make an accurate arrest for every crime and most crimes never result in arrests. Our record of past crimes is really a record of crime reports and law enforcement actions, which is too often forgotten. It has big implications when it comes to the fairness and ethical implications of these tools, because it turns out that very often the choice to predict arrest rather than crime has important consequences for racial equity, for instance. I do not want to pre-empt further questions, but I want to flag this. This is at the root of the problem: the fact that we have to use proxies. Instead of crime we use, for instance, arrests, and that will be skewed. It will be a skewed proxy many times.

Q4 **Lord Ricketts:** Thank you very much. Professor McCartney and then Professor Raab,

can you also weave in this issue about bias and the risks of bias in the design or in the datasets that are being used? Colleagues will come on to this, but perhaps we can get that issue on the table as well.

Professor Carole McCartney: I will make a couple of points. Without repeating my first answer, again who knows? Who can answer that question? I certainly cannot answer that question. As Professor Delacroix states, you could not answer the question generally anyway because it would depend on each technology as to whether it is reliable.

What we do know, of course, is that one of the big criticisms of technologies, which we have been using for many years now—a lot of forensic technologies, a lot of biometric technologies—is their lack of scientific basis. Time and again reports will come out. The House of Lords did a report on forensic science recently and concluded that the underlying fundamental research is often lacking, and there is nothing new here; very often a lot of these technologies will be based on very sketchy scientific foundations, and that is dangerous.

Another issue is who is collecting the data that would be able to tell you whether or not these things worked, because the data to gauge accuracy, reliability or validity needs to be collected and analysed, and that is not happening. We have had trials, such as the South Wales Police trial on automatic facial recognition, and I think it is very problematic that these were labelled trials. Essentially, they put the technology out into the wild and just keep an eye on it, and they call it a trial. That is not how scientific trials work.

To make a last point, of course validity and reliability are an important issue. The technology might not work, but if we think that the technology works and it does not but we cannot tell, that is even worse. Accuracy is only really one part of the question. I know you will have lots of other questions and there are lots of other issues, but with automatic facial recognition a lot of onus is put on the accuracy rate or the false positive rate and so forth. That can take us down a route where it all becomes about accuracy. There are far more questions to ask about whether we still want to use the technology even if it does work.

Lord Ricketts: Absolutely. My colleagues will come on to all those points, but an initial building block is whether it actually works, and from what you have been saying it is very worrying if the scientific rigour is not there. Professor Raab next, please.

Professor Charles Raab: I agree with what my colleagues have said. There is the question of why they do not work or what they work better than: that is to say, what are the alternatives that may be less intrusive, less expensive, more effective, more efficient, and more just? What are the criteria for “working”? You set a threshold for working or not working; but it is not really a binary switch. It is very hard to measure, for the reasons given.

There is little researched evidence for the claims that are made for either their success or their benign qualities. Equally, there is very little systematic research evidence for the alleged drawbacks and injustices, and that sort of thing. The results of research vary because they are taken out of context. Much of the research is on the USA, particular cities in the USA or other countries. There is therefore an inference that it might work over here, but that is not necessarily a justified inference. It depends on the data that is used. It depends on the analytical models that you apply to the data and the variables that you choose to put into the model. It depends how you set the risk levels, the thresholds and so forth, and what police action is taken after the results of the application of the prediction come in from the back room.

There are a whole range of reasons why it is very difficult to do valid research on this, and it is very difficult to do experiments. I wish there were more and better research, but we have not reached that stage yet.

Lord Ricketts: That is fascinating. Thank you.

Q5 **Baroness Pidding:** Thank you to all our witnesses. Gosh, what a minefield this is, which we just get from the opening statements from our witnesses. Overall, what benefits do we see these technologies bringing and to whom? Do you see that those benefits outweigh any of the pitfalls?

Professor Carole McCartney: That is a great question, of course. It almost follows on from what Professor Raab was saying, inasmuch as it depends on what benefits you think that you will accrue and what success looks like. One of the difficulties in this area is that there is no silver bullet. There is no technology that will come along and solve domestic violence or enable us to predict burglaries successfully 100% of the time. Then you have to bring your expectations into play. That is a decision that we all have to make: how much money, time and effort are we going to invest in this technology, because, of course, that will take time, effort, and resources away from something else, and then what do we expect in return for that investment?

In my research, I have focused particularly on the DNA database. It has been around a long time. It is scientifically valid and reliable. Millions were poured into it. We had lots of human rights issues around the DNA database, but as a society we have agreed that we will have a DNA database; we will forgo some of our rights, and if you are arrested and convicted you will be on this DNA database. If you ask what we are getting out of that DNA database, for a start it is difficult to know because the data is not collected particularly well. We have broad statistics about how many people are on it but it is very difficult to get a handle on.

There is one broad statistic that you can look at. If you look at all the crimes that we suppose happened during the year, the DNA database helps ‘solve’ around 0.3%. That is something that we rely on, that is accepted, that is scientifically valid and reliable, and that is the outcome we have from it. Obviously, it is more successful in other cases, and you can use anecdotes and say, “Yes, but we caught this person”,

but then, of course, you can also ask why it was not successful in all these other cases, and so forth.

A lot needs to be done to make sure that the technology works. If you bring in a new technology and say, "Okay, we've got this new technology", you have to have all the other parts of the process working in order to make that technology work. My favourite line is from some researchers, Leary and Pease, who said that the DNA database is like a great sandwich filling, but there is still stale bread because the policing is not working, the prosecution does not work, the courts do not work. You can get a DNA match if you are lucky, but none of the rest of it works, so it nullifies any impact you can have from that technology.

There are no silver bullets. You have to have an expectation of what you think this technology will achieve and decide what you are going to sacrifice in the resourcing of other things in order to achieve that. You might get from what I am saying that I am a bit sceptical.

The Chair: We do not need to hear all our witnesses' scepticism, but I think that Professor Raab wants to add something.

Professor Charles Raab: Yes. I would like to focus here on the claims that are made for the benefits in a variety of areas. We might want to separate these from each other. One is solving crimes or, if you like, forensic uses; we heard a little bit about DNA there. Preventing crimes is another possible benefit. As we have said before, we do not yet know whether it really does. Finding missing persons is another claimed benefit; we need to drill down to see to what extent that has been a helpful use of technologies. The maintenance of public order and crowd control at large gatherings and so on is very controversial, but again there is a claim there that it has an effect on maintaining public order.

The opposite view is also important: that in fact it disrupts some other senses of what public order might be by using drones or CCTV and so forth. There are also claims that it leads to better economy, better deployment of police resources, efficiency, and effectiveness. Very often, because some of those things can be measured in pounds and pence, they tend to take precedence over the other benefits that are claimed.

We need to disaggregate the idea of benefit into the different uses for which different technologies are being developed.

The Chair: I can see that Professor Delacroix wants to come in. I knew that it would be impossible to keep to time on this. We might just take one witness for each of the subsequent questions unless others have lots to add. I am sure you have a lot to add, Professor Delacroix.

Professor Sylvie Delacroix: I will try to be brief, but I thought that I should mention this: who does it benefit? Professor Raab mentioned the fact that it can benefit the general public if public resources are better used as a result, and these are big "ifs".

One study that caught my eye, which I think is interesting in terms of also addressing the ethical problems that we are going to talk about, is that there have been trials to use what epidemiologists call—well, I will not use the technical terms. Basically, there are studies that argue that murders, for instance, spread through social networks following an epidemic-like process. We are all too familiar now with these epidemic-like processes. Similar studies have been conducted for gun violence and things like that. What has been very interesting on that front is that there have been attempts to then nominate community members as preventive community-based interventions, in the sense that the people who are nominated by the community act as mediators and try to talk to people who are flagged as likely to be involved in the next wave of, say, gunshot violence or murders.

It has been a very interesting field of study, and I wanted to flag that once you start going away from the simplistic picture of predicting who will be arrested next, (and trying to be there and deploying forces at the right time and at the right place), once you switch from that particular objective, which is problematic in many ways, to a different objective, which is, "What can we learn from our past?"—we know that our past is biased, that is racially skewed in that unfortunately our police forces do arrest people of colour in a way that does not reflect the actual incidence of crime proportionately, so there is a racial bias there—what do we do if we learn that from our past?

These machine learning models effectively reflect our past. They are like a mirror, and either we skew the mirror and try to erase from the data we have at our disposal elements that are deemed to be unsuitable or objectionable, or we switch our approach and ask what we want to learn from this past. Maybe the answer here is how we can make it less likely that crimes take place in certain communities in a way that follows these epidemic-like patterns. That is an interesting route for study and for further debate, which I wanted to flag at this stage.

The Chair: Thank you very much.

Q6 **Baroness Primarolo:** Good morning. Before I ask my question, I draw attention to my interest in the Lords Members' register of interests, in that I am a non-executive director of Thompsons Solicitors.

This is quite a broad question, which goes to the heart, I think, of using these technologies. It is what we call the ethical concerns associated with the development of these new technologies. In particular, I am thinking of the databases which they attempt to use and which many people would consider to be private, and of all the problems that Professor Delacroix just identified about them being built on a historical view that is already skewed in its own right. Could I ask each of the witnesses to put on the record what they consider to be the main ethical concerns, basically the trade-offs, that we need to consider as we look at the developments of these technologies?

Professor Sylvie Delacroix: If I had to pick one concern—it is also a call for action at the same time—it is that at the moment we simply do not have the level of national

debate that would make it possible for us to ask ourselves what we want to learn from the past that is revealed to us through those predictive tools. We are getting information about patterns that we were not aware of before. What do we do with this information? That is something for which we need a community-based debate. There are opportunities. There are things that we could do constructively, but they require way more transparency and a systematic recording of choices as to which data have been used and which assumptions have been made in the proxies that are used for crime and so on.

The Chair: I will go next to Professor Raab, but it might be helpful if I remind our witnesses that they can follow up in writing on any of the points that are being made, and that can be part of the evidence that we are taking.

Professor Charles Raab: I will try to be brief. Baroness Primarolo referred particularly to databases and data sources. A pretty good start is to look at data protection law and the principles within that, although that certainly does not cover all the ethical issues: the risk of harm to the rights of individuals; the harms to society more generally; the question of the necessity and proportionality of the use of data; the question of discrimination through the uses of data; and the ethics of using particular sources of data, such as scraping social media for various purposes, particularly if those things are not transparent and if there is a lack of accountability in the use of certain kinds of data sources, possibly because of the nature of those data sources, partly because of operational issues in the law enforcement world.

I would start with the data protection side of it and look for the ethical concerns there, but I would not stop there.

Q7 **Baroness Primarolo:** Thank you. I would like to drill a little deeper with the witnesses. It is a public session, so could they specifically flag up areas of concern, notwithstanding the point that Professor Raab has just made, quite rightly, about data protection, and the fact that that could be breached? We have touched on bias and discrimination. I can think of a list, but I would like to hear the witnesses' views on what that list would look like and the danger of a breach if there is not the transparency, accountability and public debate that has rightly been flagged up. Perhaps Professor McCartney could touch on what this involves, because she has made very clear her views on the question of proper debate, as have others.

The Chair: Before Professor McCartney comes in, I will have to ask you to do it in a pretty telegraphic sort of way, because otherwise we will go on until the middle of the afternoon. I would like to do that, but we cannot.

Professor Carole McCartney: Yes, I will be very brief. Professor Raab has already mentioned discrimination. We have issues of self-fulfilling prophesies perhaps, and feedback loops in particular, where people will get caught in a system. That might change or alter policing and then, of course, it magnifies discrimination of different populations. That is very serious.

We need a human rights focus. You could give a list of principles. Baroness Primarolo said that she had a list of issues. There are things like consent, which is very important. Have people consented to have their data used in these ways?

The difficulty is that you could give a checklist of ethical principles, but it will all depend on the context and that particular technology. What you cannot do is just have a toolkit, a generalised thing that could blanket across every technology. You have to have a really sophisticated view of the technology, where the data is from, what it is doing, why it is doing it, who might benefit, who will be affected by this, and a very nuanced view. We have legal principles. We have human rights. We have data protection laws and so forth, and we have a series of ethical principles, but it will all depend on that specific context and that particular technology, so I am afraid I could not give you a list of the ethics that will be involved.

Professor Charles Raab: In the interests of brevity, I will simply say that I endorse that. It is not a question of throwing a set of principles at an issue, whether these are data protection principles or ethical principles. It is a question of context.

Professor Sylvie Delacroix: On the transparency front, I just want to add that, interestingly, the opacity of these deployed algorithmic systems is a concern. In the United Kingdom we have the data portal, the data.police.uk portal, which is interesting because datasets on crime prevalence and arrests for the UK can be consulted. The problem is that there is no transparency in the building and general designing of the algorithmic tools that are using these datasets and, what is sometimes worse, these tools are made by commercial third-party vendors with even fewer incentives to be transparent in the way that should be the case in the criminal justice system.

Q8 **Baroness Sanderson of Welton:** This is a fairly big question, but I realise that we have to be brief. How much decision-making power should we be granting to automated processes? In particular, the black box processes, which essentially take on a life of their own, feel very unsettling to me. Could you give us your view on this area and why you think it could be problematic?

The Chair: Shall I suggest that Professor Delacroix leads on this and the others come in if they have anything they want to add?

Professor Sylvie Delacroix: The black box issue is at the root of a rapidly growing field in interpretability. One of the things that practitioners in this field are trying to design is ways of relying on either transparency strategies or post hoc explanations to try to get rid of this black box idea. It is true that machine-learning algorithms work in very different ways from decision tree systems, but there are ways of getting meaningful feedback from machine learning systems. It is a design choice. You can design these systems in a way that allows for interaction and even sometimes contestability, which is extremely important.

Interestingly, research on this front is way more advanced in the medical domain, where medical practitioners have made clear that they do not feel comfortable

relying on these machine-learning tools unless they can not only ask questions but provide feedback to the system. This is very much an ongoing hot field of research. When it comes to these predictive policing tools, it is essential that we have this interaction and contestability that allows members of the police forces and members of the public to provide feedback to the system. This is not an easy fix by any means, but there are ways of building systems in that way, and it is essential that we emphasise their importance.

Professor Carole McCartney: There is this notion that algorithms or AI could replace human decision-making. Of course, that should never be contemplated. The difficulty, obviously, especially if commercial actors are designing these things, is that the humans using them have to fully understand how they work, because they have to be able to trust in the outputs. You can only trust in the outputs if you understand what the inputs were, how the system is working, what it is doing and why it has reached the result that it has.

You also have to have a human override function at some point, because if the humans do not understand the technology and how it is working, how will they spot if it has failed or if they have made a mistake? Technology might always make a mistake; nothing is foolproof, because humans have made the technology. There has to be a human override button. The humans have to understand how it is working in order to be able to spot the times when they need to not trust the technology.

The Chair: We use a technological term, do we not—human override button?

Professor Charles Raab: Picking up on Professor McCartney's point, it is very dangerous to defer to automated processes, because in the law enforcement world these tools were meant to assist human decision-making. But there may be a culture of deference to technology, particularly because the unexplainability or the uninterpretability of the algorithms might lead people to simply defer to it: "who am I to question the results of a scientific process?" It is a question of how to inculcate, in the training and in the operations of law enforcement, a sense of the ability to challenge and seek more explanations before simply endorsing what the outcome of the algorithm happens to be.

Q9 **Baroness Hallett:** The issues raised by the question that I intended to ask have been covered to an extent, so I will slightly change my question. I should declare that I was a judge for over 20 years, so I got used to the idea of technologies being used in the investigation and prosecution of alleged offenders. I remember well how in the courts it took a while for the lawyers to catch up with how you use the statistics in DNA evidence, for example. That took some understanding before the lawyers who were presenting the evidence understood the impact of the evidence they were presenting, so I do understand some of the difficulties.

My question for the experts is this. In headline terms, what would you say are the main areas this committee should be focusing on to ensure that new technologies are properly deployed in the justice system and law enforcement without impacting

adversely on the justice system as a whole?

The Chair: Does Professor McCartney want to start on that? It is a question for a thesis, I think.

Professor Carole McCartney: It is. If there was one thing that I would hope somebody grasps very soon and very quickly it would be responsibility. Whose responsibility is this? Who will take responsibility for this? We all know, and I think we can all agree, that this needs monitoring. It needs regulation. We need to have accountability and transparency. We need to have ethics groups. We need to have all these things. We have codes of practice, frameworks and guidelines now spinning around all the time. The EU is doing things in this space. We have other countries coming out with frameworks and documents. We have regulators for biometrics. We have a new one coming in Scotland. We have a forensic science regulator.

Where are we going to look to find who will set up accountability, who will keep monitoring this space, where the guidelines are, which guidelines need to be followed, who will enforce them? You can write codes of practice until the cows come home, but it does not matter if no one is taking any notice of whether people are respecting them.

There are lots of processes that need to be put in place, and we have lots of different bodies and organisations. Police are awash with different organisations. Where will we look to for who is taking responsibility here to sort this out?

Professor Sylvie Delacroix: I just want to flag this. It is dangerous to jump to legal questions when you have not solved or properly addressed the ethical questions. In this case, the elephant in the room is what we want from these tools. They are good at revealing patterns in our past, patterns of arrest, patterns of violence, and so on. What do we do with this information? That answer has not been debated or articulated with any rigour, and I feel quite strongly that we cannot move to accountability, transparency and all these things that are especially important until we have addressed that very fundamental question of what we want from those tools.

The Chair: Thank you. We may be able to answer the question by the end of this inquiry.

Q10 **Lord Dholakia:** I declare my interest as a trustee of the Police Foundation.

I come back to the brilliant principle established since 1829, which is policing by consent. This calls on the police to recognise that the power of the police "is dependent on public approval of their existence, actions and behaviour". Do the public approve of the use of the new types of technology? In particular, there seems to be considerable objection to facial recognition technology. I think that Professor Raab touched on this issue earlier on and he may want to elaborate on that.

The Chair: Yes, trust, Professor Raab.

Professor Charles Raab: The quotation in the question is, if I may say so, not complete, because at the end of the phrase "actions and behaviour" it also says "and on their ability to secure and maintain public respect"; "public respect" is in italics.

Public respect for the police is often very much in doubt, both institutionally and in the streets, so I think that that particular Peelian principle depends upon how the police and law enforcement authorities generally seek to maintain public trust and public respect.

It is a question then of what we mean by trust. We have to talk about trustworthiness. How can trustworthiness be demonstrated by law enforcement? Then trust in what? Trust in being efficient? Trust in being courteous? Trust in using technology responsibly, or what? We have to again disaggregate the concept of trust for this. The survey evidence, for what it is worth, shows that approval of the police acceptance of the technologies varies among sections of the population, at different times, in different contexts.

It is difficult to say whether the public approve of the use of new types of technologies. I do not think there is clear evidence that they disapprove but that they want it to be used within certain restrictions of fairness and justice.

Professor Carole McCartney: The important point that Lord Dholakia is making about public engagement and public consent for policing is that the police will never get away from the fact that they need public co-operation. Most crimes are solved by the public. You have witnesses and informants; they tell the police what happened. If the police move further away from that fundamental truth, believing that they can use technology instead of public engagement, being with communities, understanding communities and so forth, it could have a very detrimental effect on the relationship between communities and the policing of those communities.

Also important is what mechanisms we have for assessing the social acceptability of these technologies. Very often they are rolled out and then become controversial, and then people have to go to the courts and so forth. That is very lengthy way of doing things and costly in terms of public trust. We should not be going to the Supreme Court to see whether automatic facial recognition should be allowed. It is a ridiculous way to do things.

Lastly, there is the issue of policing priorities. What do the public want the police to be doing and to be expending their resources on? Is it just 43 individual police forces deciding, "In our force, we're going to use this technology, because this is a problem for us in Nottingham"? Then you go to Manchester, and they will be using different technologies because they have decided that there are different things they want to do in Manchester. I would find it very worrying if we had 43 forces deciding what should be done, what technologies should be used, and so forth.

There has to be some engagement with the community that is built on trust, and we should be careful with the technology if we think that we will circumvent the public in that way.

The Chair: That leads on nicely to Baroness Chakrabarti's question.

Q11 **Baroness Chakrabarti:** It really does, Chair. Congratulations to colleagues who put our questions together in this order, because we are honing down to the nub of certain issues here.

My question is about public involvement, going back to what Professor McCartney and others have said about a lack of adequate public involvement in the authorisation of these technologies in the first place and the ongoing use and monitoring of them. How should we be organising this public involvement in the authorisation and framing in the first place, and the ongoing monitoring, in order to improve trust in the justice system? Perhaps we could go back to Professor McCartney, because she is on a roll on this point and she might develop it further.

Professor Carole McCartney: I am a bit worried that I gave that impression. The West Midlands Police ethics board is quite a good model to look at, because it has been quite effective in this space already. It has quite a broad membership, so there can be some engagement with the public in that forum. Of course, we have police and crime commissioners, who are supposed to be engaged with the public in setting policing priorities and so forth.

The issue is how you would get a national view on how society would like policing to develop these technologies. We can do all sorts of research. The Ada Lovelace Institute has done a recent citizens' inquiry. There are lots of different institutes around that are engaged with the public on these issues. The difficulty is what they are feeding into. We can have these bits of research, we can engage with the public, we can do surveys, but where do we deliver the results? Who is receiving those? The difficulty is that, yes, we can try to engage public views and attitudes, and some organisations are doing that, but then we get a report at the end of it and where does it go? I am worried that there is nowhere for that to feed into.

Professor Charles Raab: I would say something quite similar. What has been especially useful are the various civil society groups that have elevated these issues into public debate, and organisations that have more of a think tank nature, like the Ada Lovelace Institute and RUSI, which Lord Ricketts mentioned. The problem with public engagement is what you do when you test public opinion on things and there is some dissonance between public opinion and what might be regarded as the ethical approach to the use of technologies.

It depends how the public engagement is being organised and what kinds of public engagement there are. Citizens' juries can be especially useful. Citizens' assemblies, or whatever they might be called, can also be useful. I do not think that survey results are particularly helpful, but it is a dilemma. We need to have some kind of debate about the techniques of engaging the public rather than simply saying, "We don't know what to say, so we'll ask the public", and then the public come up with a

divided opinion about a particular technology. It depends how you construct the public and how you bring members of the public together to debate these things.

Baroness Chakrabarti: Forgive me. I should have said before I got carried away that I was director of Liberty, the National Council for Civil Liberties, for many years and I am currently on the council of JUSTICE. That was all.

Professor Sylvie Delacroix: When it comes to public involvement, there are measures that the Government need to take to make that public involvement meaningful in the first place. For that I will go back to the recommendations that were made in the Law Society report on algorithms in the criminal justice system. The most important in this particular instance is that there should be a national register of algorithmic systems so that every algorithmic system that is used, particularly in the criminal justice domain, should be deposited and audited regularly.

There should also be both individual and societal explanation facilities. By "explanation facilities" I mean ways in which these algorithmic systems in criminal justice can be interrogated or designed to help individuals and users to assess whether a given output is justified and whether they should seek a remedy through the courts, for instance.

That is the individual aspect. It is important not to forget the more collective aspect. There are ways of facilitating or designing broader internal and external scrutiny to allow, for instance, access to the general design, functioning behaviour and impact of the models that are used by these algorithms. Here, my key word is that we have no accreditation for the moment. We have no obligation to deposit these systems in a national register—it could be the British Library, for instance—and we have no dispositions that make public interest access possible. It should be possible for public bodies in the criminal justice system to have access to these systems and research them on behalf of the public if each member of the public cannot have access to them.

Q12 **Baroness Shackleton of Belgravia:** What do you see as the main issues with the legal framework for the use of new technologies in law enforcement, both national and international?

Professor Charles Raab: The main issue with the legal framework is the need for greater clarity. Let me take the idea of data sharing, for example. Data sharing needs to have greater clarity about the kinds of data that are shared, between whom and who else. There is a lot of work being done on this at the moment, but more clarity on that is needed.

We also need more international co-operation and harmonisation in cross-border police co-operation, for example. The definition of crime may be different in different countries. Therefore, it may be more difficult to use data or to combine data for those sorts of purposes. It is also not clear what data used for a "law enforcement purpose" is, to quote a phrase that is used. A law enforcement

purpose is a very fuzzy term, and this is one of the things that is being talked about in the ICO's code of practice, which is now out for consultation.

There may also be a need for technical standardisation of different kinds of technologies. The IEEE, the Institute of Electrical and Electronics Engineers, and many other groups are working on standardisation, which would feed into the definition of many things in the legal framework.

Finally, one needs to look at what kinds of international protocols there might be to put data sharing and interchange on a legal basis. I am thinking here of Europol, the Prüm agreement, Interpol and so forth.

Professor Carole McCartney: There are a couple of points to be made further to Professor Raab's important points about clarity.

There are legal principles that can be applied. Again, it is almost like ethical principles in that it is highly contextual. There are tests, such as whether it is necessary and proportionate. You can go back to the classic Marper case at the European Court of Human Rights, which looked at the DNA database. The Government said, "Yes, It's necessary and proportionate that we have all these people on the DNA database, because we're addressing crime". They deemed it necessary and proportionate. Of course, there was an opposition view, which won.

The difficulty with necessity and proportionality is that they are questions of balance. You can have a view on what is necessary and what is proportionate, and we need to have data and evidence to support the arguments as to whether something is necessary or proportionate. It is all contextual. You would still need data transparency to be able to answer questions which the law would raise. That comes back to enforcement. There are legal principles, but who is overseeing these and ensuring that these technologies are upholding human rights and adhering to these legal frameworks? The difficulty is that laws are there, but who is checking that they are working?

Q13 **Baroness Shackleton of Belgravia:** Supplemental to that, are any of you concerned that data in the wrong hands is very scary? Information used effectively for what it is intended to be used for is valuable. It is even arguable whether it is useful or not, but certainly in the wrong hands it could be extremely damaging and it could be weaponised. What regulation do you think is proportionate in the national, regional, or global field to make sure that it is being used appropriately?

The Chair: I am not sure I have volunteers for answering that. It may be one of the things that we will have to keep on the list.

Professor Carole McCartney: I could say one thing. Regulation is the big question here: how do you regulate this? I was hoping that your committee would answer that question. It is interesting that you talk about data falling into the wrong hands, and you could argue that the question whether data is in the right hands depends on whether we trust the police and what they are doing with it. We have already seen this with the Gangs Matrix database. Amnesty International and several groups

came out and complained about that, because it was seen as unethical and that the police were not protecting this data properly and should not have been collecting this data.

We know that the police are often perhaps not the best placed organisation to be dealing with large amounts of extremely sensitive data, and we have the difficulty, the complication perhaps, of the commercial sector. In forensic science, we have a commercial marketplace and there are lots of concerns, and protections that need to be put in place so that we ensure that that marketplace is regulated and does not have access to sensitive data.

Asking whether data could fall into the wrong hands does presuppose that there are the right hands. Yes, it is a particular concern, but I think we should be concerned even if it is the police who have this data.

The Chair: Still on this subject, and perhaps Professor Raab can come in first, let me go to Baroness Kennedy.

Q14 **Baroness Kennedy of The Shaws:** I make my declaration of interest in that I am a practitioner at the English Bar and have been for many decades. I am the president of JUSTICE, the law organisation. I am also the director of the International Bar Association's Human Rights Institute.

I want to home in on a regulatory framework. If at the end of this we were to suggest that there was a need for better regulation and legislation, the question I would want to ask is: in this space, what is it that we need to ensure? I could probably start making a list, and I think you all have indicated that there are issues to do with protecting human rights, avoiding discriminatory practices, seeking to be fair and just, and so on. Are there other things that you think we should be seeking to produce in creating a regulatory framework?

Professor Carole McCartney: Obviously I have views on lots of things. One thing that I always come back to is integrity as a core. The courts have to have integrity; there has to be integrity in the justice process. Integrity is the thing that we need to ensure, and if we have integrity we should have trust and so forth.

For me, it boils down to three essential elements. First is the viability of a technology and how it works. Is it reliable? Does it have validity—this is where we started this conversation—and what standards are there? Is there quality assurance in place? That is almost the scientific leg of it.

Then there is the lawfulness leg. Is it legitimate? Is it lawful? Is it human rights compliant? Does it adhere to data protection rules? Are there enforceable boundaries so that we can protect this data? Is it necessary and proportionate?

So we have the science, and we have the law. The third element is what I call acceptability—whether it is acceptable to society. Have ethical considerations played a role? Is it ethical? Is there oversight? Is there accountability and

transparency? Is it cost-effective, as in: have we decided that we will resource this technology over and above other things we could do?

There are lots of different regulatory frameworks that you can look to. People seem to like this trio. In Scotland, they talk about lawful, effective, and ethical. There are other systems in place that other academics have come up with, but they are the three fundamental elements that I think you have to get right: is it viable, is it legitimate, and is it acceptable? Any regulatory framework, if it misses one of those strands out, is missing an important element and would not work, I do not think.

Baroness Kennedy of The Shaws: Professor Delacroix, you said that ethics have to come before law. Would you like to add to what Professor McCartney has said?

Professor Sylvie Delacroix: What strikes me here is that we are at a particularly important junction. Depending on the result of the debates which I hope will take place thanks to this committee, these tools could be designed in a way that is positively harmful for society and reinforces patterns of discrimination, or they could be designed in a way that benefits the communities that are currently discriminated against by intervening preventively, for instance.

A debate needs to take place as to what we want, and there are now studies that show that you can change your understanding of the aim of police intervention. When you change that understanding, you can design interventions that are positively beneficial for communities that would otherwise find themselves in a pattern of repeated discrimination.

When it comes to the issue of discrimination, given the fact—and nobody would dispute the fact—that these algorithmic systems have a high potential for socioeconomic discrimination and, given the fact that the Government should assess the extent to which we have the capacity to undertake the socioeconomic equality duty that is part of the Equality Act 2010, these are duties that can only really be undertaken with a capacity to grasp the system, and that will be resource-intensive. At the moment, there is a clear worry that we do not have the resources necessary to address the potential for harm and the duties that should be taken very seriously if we are to address these potentials for harm.

I wanted to flag that there are many ways of augmenting capacity. People have mentioned the Centre for Data Ethics and Innovation, for instance, as one potential body that could be strengthened. Everybody knows that the ICO is rather stretched at the moment. There is the abstract argument, and then there is the very concrete debate about how we give ourselves the means to live up to our responsibility when we design these tools in a way that should not mean that these discrimination patterns continue for ever.

Q15 **Baroness Kennedy of The Shaws:** My supplementary is about the changing nature of this technology, and it does so with such rapidity. How can regulation or law keep up? How do we do that?

Professor Sylvie Delacroix: I should let my colleagues step in.

The Chair: I suggest that we go to Professor Raab, and perhaps if our witnesses have further points that they would like to make, they can follow that up after this morning, because we still have a little way to go.

Professor Charles Raab: There are some choices to be made between generic regulation and technology-specific regulation. It is difficult, however, to find reliable technology-specific regulation, because if, as Baroness Kennedy is saying, technology is moving very rapidly, which is true, the temptation may be to say, "We need to have a law for computers, a law for facial recognition, a law for XYZ". I think that would be the wrong route to go down. If you go down the generic route, then it is a question of how you translate that into the specific context and the specific technologies that people—the policeman on the beat, the person who is trying to detect financial fraud, or whoever—need to know. That is difficult to get from overarching law or overarching ethical principles.

You need some kind of relationship between those two, and that is not easy to get unless one talks about the purposes and the particular activities that one is trying to regulate, rather than the technologies that are used in the processes for achieving those particular sectors, such as detecting online harms or predicting particular kinds of crime.

The Chair: Thank you. I will go to Lord Hunt now, because I want to give members time to ask burning questions that they may have before we have to finish the meeting.

Q16 **Lord Hunt of Wirral:** Declaring my interests first, I am a partner and practising solicitor with the commercial law firm DAC Beachcroft, and I am a member of the Law Society and Honorary Bench of the Inner Temple.

I want to turn to Professor McCartney first. I recall that she said that it is key to find out whose responsibility this is, and she mentioned all the different police forces. We do not have an exhaustive list of what technologies are being or have been trialled by all those police forces, so how could the use of new technologies by law enforcement be effectively monitored?

Professor Carole McCartney: We have national organisations. For example, you could automatically think of the College of Policing or the National Police Chiefs' Council, the NPCC. They should have a national purview of what is going on in all the different police forces. Perhaps you could look to their national bodies if you were looking specifically at policing technologies.

We end up with this quandary about national regulation versus local regulation and at what level we want the regulation. I think the NPCC needs to play a role here. I am loath to suggest that there should be a separate organisation, because you create another organisation, and we just end up with more organisations. The NPCC would be my first go-to for getting a national view of what is going on and it having some responsibility for it, even if it is to impose some local regulation that the 43 police forces would have to have independent monitoring that then fed into that national level.

Q17 **Lord Hunt of Wirral:** Thank you. Turning to Professor Delacroix, you have just talked about positive benefits for the community. I suppose what the community wants to do is to live our lives without fear, walk our streets and so on. The motor car, though, still kills large numbers of people. The police rely on various mechanisms, but we now have private companies that are developing some tools. We referred earlier to black boxes. The trouble is that those private companies are not sharing details of their technologies for audits on data privacy grounds, so how will we deal with that, given the positive benefits for the community of a more coherent approach?

Professor Sylvie Delacroix: I have no doubt, and I will repeat myself here, about the need to have a national accreditation system and a national repository, an obligation for any algorithm that is used in the justice system to be deposited in a national repository, which means that they can be audited regularly, and they should be audited regularly. These commercial companies should not be able to hide behind these kinds of data privacy concerns in the sense that once you have a national repository you allow certain entities to audit or have access to these algorithms on behalf of the public. Otherwise, it is quite simple; you should not allow these systems to be used in the criminal justice system. That is a no-brainer, in my view.

If you talk of benefits, you cannot talk of benefits lightly. You can only talk of benefits if you are prepared to ask difficult questions about what exactly we want our police forces to be pursuing. At the moment, we have insights into patterns of activities, patterns of criminal victimisation. We did not have these insights before. These insights can be used not just to deploy forces where we deem it likely that there will be crime but to change the factors that create the likelihood of crime. It is quite a different approach, whereby you acknowledge the fact that there are social and educational factors, all sorts of factors, that will make it possible to predict these crimes and what should we do about it as a society.

I do not think that the only answer is to deploy a police force. The answer is much more complex. It is an intervention that involves social services, educational services, and so on. It is about how ambitious we want to be with the data and the insights that we now have at our disposal. That is a wider question, but it is a question that needs to be considered at the same time if we are to legitimately say that there can be a community benefit.

Q18 **Lord Hunt of Wirral:** Finally, to Professor Raab. I am never quite sure what algorithms are. I suppose they are a sort of finite sequence of well-defined computer-implementable instructions, but against the background of what we have just heard, Professor Raab, how does that equate with your principles of fairness and justice, which you spoke about earlier?

Professor Charles Raab: At this point I might have to reach for my textbook to give you a definition of AI. It is a question of which textbook I reach for, because there are so many of them. However, in my understanding of it, which is not at an extremely high level, there may be fairness or unfairness about the way in which

the data on which an algorithm is trained has been collected, the composition of that database, and so forth.

For instance, it has been shown that ethnic differences go into the collection of data on which certain policing algorithms are trained, which creates certain kinds of bias in their application. There may also be biases, or rather the results of judgments, in the development of the model for the algorithm, judgments about where to put certain thresholds, how to assess risk, and so forth. The algorithm is not a kind of magic bullet that cannot be questioned. One always needs to question whether the algorithm itself is fair in its modelling of what it is doing and whether it is fair and just in terms of the data that went into constructing the algorithm. That is a short and not terribly learned answer.

Q19 **The Chair:** My next question is to Professor Delacroix. Your work for the Law Society on this area. Have the Government responded and, in particular, have you had had any response or follow-up to your recommendation—this is probably more broadly topical than to just this issue—on the commencement of Section 1 of the Equality Act, the public sector obligation regarding socioeconomic inequalities, which seems to me to be relevant to what we are talking about now. As there are now five hands up, if your answer is no, that is fine.

Professor Sylvie Delacroix: The answer is no. If there has been any response, I am not aware of it.

Q20 **Baroness Chakrabarti:** I am following up on some of the most recent evidence from witnesses about the underlying purpose of the criminal justice system, let alone the technologies in the system. To what extent is the current malaise that you are describing reflective of the blurring between intelligence, policing and criminal justice outcomes in terms of penalties and, indeed, between civil and criminal law in recent years?

The Chair: Can one of you try to answer that question? Professor Raab?

Professor Charles Raab: I may not be able to answer, but I can add a further thing. There may be a blurring between police activities and counterterrorism in ways that impact upon the situation that Baroness Chakrabarti is describing.

Baroness Shackleton of Belgravia: In my flunking with the machinery, I did not declare my interests, which are that, as a solicitor, I am an Honorary Bencher of Inner Temple and I am a member of the Law Society.

The Chair: I am sorry. I should have mentioned it myself.

Q21 **Lord Ricketts:** We have had a very UK-based discussion. Do any of our witnesses have any examples of good comparators overseas that do the issue of regulating and overseeing the encroachment of AI and algorithms into law enforcement particularly well that we might look at?

The Chair: We have heard a sort of warning that the US is different. Professor Raab made that point early on. Are there any applicable examples? Again, if you would

like to follow that up after this morning, please do.

Professor Carole McCartney: The EU has written extensively about ethics in AI and is now looking to legislate in this space. There are EU examples to look to. The Australian Human Rights Commission has just published a fairly comprehensive report on the use of AI in the justice system that is well worth looking at. The Canadians as well. These are probably the usual suspects that we would look to, largely because of the complications of the US system. I would look to the Australian Human Rights Commission. I have forgotten the name of the relevant Canadian organisation, but I can fill it in in my written evidence. The Canadians have done quite a lot in this space.

Q22 **Baroness Kennedy of The Shaws:** Picking up on that, I was going to raise the issue of reports on lie detection testing that have emanated from other jurisdictions, which make quite clear how unreliable lie detector tests are. I wonder about police forces running pilot schemes using this stuff when there is evidence coming from other common law jurisdictions about the unreliability of it. Perhaps that is a question for Professor McCartney. Do the police look at the research that suggests that this is not a positive road to go down?

Professor Carole McCartney: That is a very good question. Some research into this has recently been done by some of my colleagues at Northumbria Law School. It is frankly baffling as to why polygraph testing is now being introduced more widely, particularly in the counterterrorism space, but also in probation and parole in particular. Research from across the world has shown its unreliability. It is almost a symptom of austerity. The police need to do more with less. They get sold, perhaps, on different technologies. We have seen this a lot with things like rapid DNA testing and so forth. Companies, or advocates of a particular technology, will convince police officers that they can achieve X, Y and Z for a lot less money, quickly and effectively, so "Why not give it a go?" We lack the regulatory framework that we have been referring to, so these things have been catching on, much to our consternation. Polygraph testing is a good example of some of the dangers in this area of unreliable technologies being adopted none the less.

Baroness Kennedy of The Shaws: You have just mentioned terrorism. A lot of my work in the past has been in cases involving terrorism. The great difficulty is that when you are dealing with terrorism, or national security, it becomes quite easy to promote the unacceptable because we are dealing with something that is so frightening to the general public.

The Chair: I will take that as a comment, but also remind us all that it is not just about how reliable a technology is but what questions you are seeking that it answers, particularly in the case of polygraphs.

Q23 **Baroness Primarolo:** I want to return to the point about public consent, or public understanding of what is being used. In a context where anything appears to be possible, and is being developed, do we need a prohibition on the use of these technologies until we have that first regulatory and principled overarching view? It

seems to me that it is a bit like the embryology debate many years ago, when what scientists could do and what the public understood to be acceptable were miles apart. It is perfectly possible that that is the case here. Should we have prohibition until we have a regulatory framework?

Professor Carole McCartney: We have talked about things like moratoriums. The difficulty is that very often, as I have pointed out before, trials of these technologies tend to consist of just putting them out into the wild but keeping an eye on them, and of course they are difficult to bring back from the wild. We have seen that with things like forensic phenotyping and now forensic genealogy, where people are using family trees to track down offenders and so forth. It does not take too long before you can say, "We've caught a murderer using this technology. Therefore, we must be allowed to carry it on because, look, we caught a murderer". We end up getting swept away with anecdotal success stories, which totally obscure all the drawbacks, problems, difficulties and so on. It is like the genie out of the bottle. It is difficult to put it back and the public can get swept away in this, as well as the police. We have some examples of countries bringing in moratoriums. We have quite a few on automatic facial recognition and also now on different forensic DNA technologies.

As far as I am aware, New Zealand—I was involved last year with its Law Commission looking at its DNA rules—is the only country that is now scaling back on DNA technologies, saying that their effectiveness is questionable: "We give up all these rights and there are difficulties with that. We don't need this technology as much as we supposed, and we're going to scale it back". I would be in favour of preventive measures, so do not let the genie out of the bottle because it is difficult to scale things back once it is out there in the wild.

Q24 **Lord Dholakia:** Professor Delacroix mentioned the adversarial relationship between black and ethnic minority communities and the police. One of the factors that has come about is that a majority of UK citizens from minority groups, for whom the technology of facial recognition is less convincing, want to opt out of this particular use of technology. How would you establish confidence in the justice system if a section of the community does not accept what is being recommended for them?

Professor Charles Raab: I think Lord Dholakia in a sense has answered his own question. How can we trust things that a section of the community finds to be discriminatory? It is a very real issue.

May I turn for a moment to add something to what Professor McCartney said? There is an example of the prohibition of live facial recognition in San Francisco, and maybe in other jurisdictions abroad that have done this. She raised the question of how you experiment with it, because it has been argued—I think successfully—that even the conduct of an experimental live facial recognition trial has consequences for the people who happen to be caught up in that trial, and who therefore are affected by it, being taken aside because they have supposedly been recognised.

If I may add a small tailpiece to this, which has not been mentioned before, the people who make, purvey, sell these technologies are very persuasive. I think there would be some benefit in looking at the relationship between law enforcement and the suppliers and salesmen, the companies, that sell this stuff in order to understand how that relationship works, and whether it is a little bit too hand in glove sometimes and whether the claims for the technologies, which are being made by those who make them, are exaggerated and the police find themselves at a disadvantage in evaluating them for procurement purposes. Thank you.

The Chair: Professor Delacroix is there anything you would like to add at this point? We have months of work to go.

Professor Sylvie Delacroix: I do not want to prolong the meeting unnecessarily. The information so far has already covered much of the answer I would like to put forward. I would just say as a concluding remark that, at the moment, what is top of mind is that we need to be very careful about the fact that there is a technical allure associated with these prediction tools. That can dangerously distort, or in some ways displace, very important moral and political debates that we need to have right now about what we want the police forces to be concentrating on and what measures, if any, can be taken to break the links that are now increasingly evident between, say, some kind of socioeconomic disadvantage in the background and the chances of being arrested later in life and things like this.

There are ways that have been shown to be effective in breaking the causal chains that lead to the predictions at the heart of these algorithmic systems. That is a question that we cannot afford to ignore when we discuss policies related to these algorithmic tools.

The Chair: Indeed, which is why I thought your point in the 2018 report about socio-economic inequality was so important.

I thank all three of you very much. This has been a terrific session. We have a huge amount to think about, and with all that assistance you have put a lot into our heads—questions if not answers; you have made it clear that a lot of the answers are missing—so we have quite a job to do. Thank you very much indeed. If there are points on which you would like to follow up, please do, and we will reserve the right to come back to you, if we may. Thank you very much indeed.