Select Committee on Science and Technology

Corrected oral evidence: Forensic Science

Tuesday 27 November 2018

4.50 pm

Watch the meeting

Members present: Lord Patel (The Chairman); Lord Borwick; Lord Fox; Lord Griffiths of Fforestfach, Lord Hunt of Chesterton; Lord Kakkar; Lord Mair; Lord Maxton; Baroness Manningham-Buller; Baroness Neville-Jones; Lord Oxburgh; Lord Renfrew of Kaimsthorn; Lord Thomas of Cwmgiedd; Baroness Young of Old Scone.

Evidence Session No. 12 Heard in Public Questions 123 - 131

Mark Stokes, Head of Digital, Cyber and Communications Forensics Unit, Metropolitan Police; Dr Jan Collie, Managing Director and Senior Forensic Investigator, Discovery Forensics; Professor Peter Sommer, Professor of Digital Forensics, Birmingham City University.

Witnesses

USE OF THE TRANSCRIPT

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

Examination of witnesses

Mark Stokes, Dr Jan Collie and Professor Peter Sommer.

Q123 **The Chairman:** Good afternoon, lady and gentlemen. Before we start could I mention two things? First, would you introduce yourselves so we get that on the record? Secondly, it is possible that any minute now we might be interrupted for a vote and, if that happens, I am afraid we will have to call a halt for a few minutes.

Mark Stokes: I am head of digital forensics at the Metropolitan Police Service, part of forensic services.

Dr Jan Collie: I am from Discovery Forensics Ltd. We offer digital forensic and cybersecurity services to corporate and legal clients.

Professor Peter Sommer: I am professor of digital forensics at Birmingham City University. I have a visiting professorship at another university. I work for both the prosecution and the defence because my professorships are only 10% of my time, given that I am semi-retired from academic life. In the past, I have been the joint lead assessor for the old system run by the Council for the Registration of Forensic Practitioners. I also sat for a while on the advisory panel used by the Forensic Science Regulator to look at digital forensics.

The Chairman: My question might seem too simple for you but it is very important for us. Could you crystallise for us what digital forensics is, how it differs from cyber forensics and what cybercrime is?

Professor Peter Sommer: There is no clear definition—

The Chairman: That helps us a lot.

Professor Peter Sommer: If you let me finish the sentence, perhaps I can help you. Digital forensics is anything that involves looking at a digital device or digital transmission. You can have arguments on the fringes of forensics. Obviously, it includes looking at computers and smartphones, looking at data in transmission and looking at large computers, but it also includes looking at more conventional or older forms of forensics, because some of those have gone digital as well. CCTV used to be purely analogue but there is now a digital element. Some of the work that you might do on CCTV would involve digital forensics, but recognising a particular face would be done using old-fashioned forensics. My short answer, which you said did not help you very much, is there are no clear definitions, and it is much more a question of what practitioners can deliver in particular circumstances.

Mark Stokes: There are some Home Office definitions, to perhaps add some clarity. If we talk about pure cybercrime, these are crimes where a digital system is targeted by means of a criminal attack. These attacks are designed to disrupt our infrastructures and include things such as DDoS attacks. Cyber-enabled crimes are those crimes which use the current internet and infrastructures to commit crimes that would previously have been committed in another way: card fraud, the use of

mobile telephones or digital systems to ask for card numbers. It is not a "cyber" crime per se. Digital forensics, to add to what Peter was saying, is about the processing of that digital data and ensuring its integrity throughout the process and the interpretation of that data for the criminal justice system.

Professor Peter Sommer: It has very little to do with cybercrime. For historical reasons, I get quite a lot of the big hacker cases, which people would traditionally think of as cybercrime. My instructions have included terrorism cases, several rather gruesome murders, trading in firearms, trading in narcotics; it can be practically anything. These days it will even include basic street crime because there will probably be some CCTV or geolocation mobile phone data involved. There is very little connection between digital forensics and definitions of cybercrime.

The Chairman: Thank you very much; that helps. Baroness Manningham-Buller.

Q124 **Baroness Manningham-Buller:** We have heard in this inquiry so far differing views on the balance between private provision of these services, in particular digital, and police provision or in-house provision. We would welcome your views on whether that balance is right today and whether, if you could and the funds were available, you would change it in any way.

Professor Peter Sommer: My personal view is that it is a mistake to outsource digital forensics other than in very exceptional circumstances. The reason for that is that if you have an inquiry it is unlikely that the immediate OIC—officer in charge—is going to have an idea of the range of possibilities that exist inside a computer. If it is outsourced, an OIC will try his best to say what he wants. If he sends it to an outsourcer who is being squeezed on price, the outsourcer will do exactly what is asked of him, but no more. The system at its most productive is if the technical investigator and the regular investigator sit down together and try to work out what the issues are and where they can stimulate each other to get a better result. There is scope for outsourcing on the very simple side and there is scope on the expert side, particularly when you want expert evidence as opposed to technical evidence.

Baroness Manningham-Buller: There are also constraints within the police budgets. It is not just the market constraints on private provision.

Mark Stokes: Fundamentally, there is only so much money in the public sector system. Whether you insource or outsource it is not the question. It is how, as Peter is implying, you manage the ecosystem in trying to get that work done within that limited budget and the constraints you have within that. I would agree with Peter, but you might think that I would say that, wouldn't I?

Baroness Manningham-Buller: I could not possibly comment.

Mark Stokes: I will let others speak. There are certainly benefits with insourcing but it is the same envelope of money; that is the point.

Baroness Manningham-Buller: What are the benefits, as you see

them, from the market?

Mark Stokes: Speaking from personal experience, in the Metropolitan Police Service we have used the private sector to do some of the more complex stuff. We still struggle with finance, but we are using a managed service provision to help us. Instead of the market throwing technologies and software at us, we are working with a private sector company to leverage those technologies and develop them for digital forensics.

Dr Jan Collie: I—

Baroness Manningham-Buller: I will come to you in a minute, Dr Collie. Mr Stokes, I think you were saying that you give the more complex things to the private sector whereas Professor Sommer was saying that you give the easier things to the private sector.

Professor Peter Sommer: No—

Baroness Manningham-Buller: Have I oversimplified that?

Mark Stokes: Yes. To clarify, what we are saying is the development of the software and some of the research and development can be done with the private sector. The actual evidential work needs to be done in unison, whether in the private sector or the public sector, with the investigative process. Bearing in mind that you have to avoid cognitive bias, it is also very important where forensic science sits in that process.

Dr Jan Collie: That—

Professor Peter Sommer: What I was saying—

Baroness Manningham-Buller: Dr Collie, I really will come to you in a minute.

Professor Peter Sommer: We have done this sort of thing before and Jan will speak up in time, I am sure. To clarify what I was saying, I think there is scope at the very simple level, but otherwise, as Mark is saying, it is at the complex level. The vast majority benefit considerably from insourcing, simply because it is important that investigators work together. If you are calling in an outside expert, my strong preference is that I go and work with the investigator. I do not want work doled out to me without having a context.

Baroness Manningham-Buller: Dr Collie, please add to this.

Dr Jan Collie: It is not what I am seeing out in the field and it is not what police officers are telling me. I was speaking to some only last Wednesday. What I am seeing in the field is that regular police officers are trying to be digital forensic analysts because they are being given these rather whizzy magic tools that do everything, and a regular police officer, as good as he may be, is not a digital forensic analyst. They are pushing some buttons, getting some output and, quite frequently, it is being looked over by the officer in charge of the case, who has no more training in this, and probably less, than him. They will jump to conclusions about what that means because they are being pressured to do so, and they do not have the resources or the training to be able to make the right inferences from those results. That is going smack in front

of the court. In my view, and I do an awful lot of this day in, day out, the criminal justice system is like some evil sausage machine that is just trying to criminalise people. Once you get into the maws of the criminal justice system, it is jolly difficult to get out. If I may, I will quote a solicitor I was working with a year ago on a rather large worldwide case, and this is important for access to justice. He said, "People come through my door certain that the legal system is scrupulously fair and I have to watch as they gradually find out that it isn't. Without exception, by the end of the trial they end up thinking that the prosecutor is a corrupt bully and that the judge is biased against them". Is that what we want?

Baroness Manningham-Buller: Rather than attacking the whole criminal justice system—

Dr Jan Collie: Sorry, but—

Baroness Manningham-Buller: Can we focus it on what you would do, if that is your view, with forensic science to improve that opinion of yours, rather than the whole system?

Dr Jan Collie: The whole system is obviously massive so you cannot improve the whole system in one fell swoop.

Baroness Manningham-Buller: This inquiry is about forensic science.

Dr Jan Collie: Money needs to be invested in training officers who are on the front line. All they are getting at the minute is about a day's worth of training, if they are lucky, on how to push buttons and get answers. They need more than that. I was talking to a police officer on an indecent images case only the other day, and I said, "First, we need to get an MoU signed", because you have to have that signed so that you can take away those illegal images and work on them so you do not get criminalised because you are working on them. He did not even know what an MoU was. I had used the word "images" and he thought I was talking about the nasty pictures, not a digital forensic image. They do not even have the basics. The people on the front line are being asked to run these tools over hard disks and over people's mobile phones—

Baroness Manningham-Buller: Is your solution to that training the police officers or outsourcing what they are doing?

Dr Jan Collie: If we are going to use police officers like that, we have to give them better training. It is very unfair to ask a regular police officer to stick his neck on the line like that.

The Chairman: Lord Hunt—

Mark Stokes: Can I come back on some of that? If we ensure that it all works within a quality management system, that is part of it. ISO 17020 and 17025, and statutory powers, have a part to play, in my humble opinion, in all that. Today, a police officer is what I would term a "digital native" when they come in, as in they use social media and are used to all this technology. However, they do not know the constraints and limitations. Training on what should be seized and how it should be handled is absolutely critical and there is a lack of that. They get taught how to write out tickets and do traffic duties and all those things, but a

core part of their police training should be around the digital world. A lot of work is going on around that with DMIs—digital media investigators—and digital intelligence and investigation. However, more needs to be done in that basic training.

The Chairman: We are coming to more of that in a subsequent question. Can I move on to Lord Hunt?

Q125 **Lord Hunt of Chesterton:** You have partly answered this question: what is the level of understanding of digital forensic science within the criminal justice system among lawyers, judges and juries?

The Chairman: You have covered some of that.

Lord Hunt of Chesterton: You have covered some of it, but how can it be improved? It sounds as if you are saying that some of the front-line people have very little training. Presumably they are talking to some lawyers, who have a slightly higher level of training, but juries also need to understand it.

Dr Jan Collie: That is absolutely right.

Lord Hunt of Chesterton: How do all these different competencies fit together?

Dr Jan Collie: It is like talking about a world over here and a world over there, because the court system is very different. The judges usually have a pretty good idea because they have usually sat on quite a lot of cases and they pay attention, and, if they are not sure, they will ask the expert while they are in the box. Barristers, likewise, tend to learn quite a lot while they are on their feet doing these cases. Occasionally they go a bit too quick into thinking they understand it to the core. As regards a jury, it depends who is on it. You cannot expect all jury members to have much idea about computers and mobile phones and how they work and that sort of thing. That is where the role of the expert is key, because without that help—and we are there to assist the court—the jury cannot ask those more fine-grained questions that it needs to drive to to come to the right answers in its deliberations.

Mark Stokes: There is a lack of consultation within the criminal justice system with the experts, and a lack of a conversation about what the evidence means, and sometimes assumptions are made.

Lord Hunt of Chesterton: Is the emphasis sometimes too much on the digital side when there is still some basic business—things I might know about?

Professor Peter Sommer: It is very patchy. You can get judges who are extremely alert. I have seen judges cross-examine an expert where they knew exactly what they were doing. You get other judges who busk their way through and get angry and annoyed because they think what is being said is irrelevant, usually because they have not understood what is going on. One of the other problems with judges at the moment is that they do not understand how to manage cases where there is digital evidence. You have to realise that the quantities are huge. It is important

that at a case management stage a judge asks everybody who is supposed to produce digital evidence, or produce reports, to state what sort of timetable they are prepared to work to and make them stick to it. The bane of everyone's life if you are in this particular game is the day before a trial, or even during a trial, somebody comes along and says, "There is this great new bit of the evidence; it is really important", and you say, "I haven't got time to do it at the level of quality you are expecting", and everyone looks down at you—"Don't you realise the expense of a cracked trial? You have the judge, all these witnesses and jury members. Please do your best". Your best may not be good enough.

One of the things we need to look at, and I hope is reflected in your report, because I know you are looking for recommendations, is that judges must have much better case management where there is digital evidence.

Lord Hunt of Chesterton: Presumably the judge's role is also, as we have discussed before, to look at the evidence and technology of the defence and prosecution.

Professor Peter Sommer: It is open to a judge to order or arrange for a meeting between experts before the trial. It is Criminal Procedure Rule 19.6. I have done a lot of that sort of work and written about it in academic journals, and I think it is enormously beneficial because very often there will be a lot of agreement between experts and you can shorten the length of the trial and not bore the pants off everybody with stuff about which there is no dispute. You will then get the experts to say succinctly, if they disagree, what the points of disagreement are. That comes down again to good trial management. It is in the Criminal Procedure Rules. You do not have to invent anything if you make a decision at the right time, at the pre-trial review, to use the method.

Mark Stokes: On that point, there is a fundamental challenge here that we have to try to address throughout the criminal justice system. The technology moves very quickly and what can be done one day changes the next day. You need open access to that information and knowledge online somehow, so that the judiciary, the CPS and others are informed of what the latest technology can do.

The Chairman: The communication side.

Mark Stokes: That can change daily.

Lord Griffiths of Fforestfach: From your experience of being involved in trials and so on, to what extent have judges in their summing up had to make a judgment regarding the evidence of forensic science?

Professor Peter Sommer: It is not their job to do that.

Lord Griffiths of Fforestfach: It may not be their job to do that but that is not the question I asked. The question I asked was: do they actually do it?

Dr Jan Collie: It is hard to answer that question because usually you have gone before the end of the trial and you do not hear it, I am sorry to say.

Mark Stokes: You sometimes get a transcript, but that is very rare indeed, and that is normally when something has gone wrong and you are going back through it all.

Baroness Young of Old Scone: Can I ask about these pre-trial meetings? Should they not be obligatory so that the experts reach agreement and a view before the trial?

Professor Peter Sommer: They are not obligatory but it is often very sensible. It can happen in two circumstances. Very often in a complex case, the experts will suggest, "Why don't we have a meeting?", and there are particular rules about how that meeting is conducted, the basic rule being that it is collegiate and the contents of the actual discussions are not disclosable. The only thing that is disclosable is what happens at the end. There is also an option for the judge to order it. My personal experience is that counsel tend to recognise the value of having those meetings, because a lot of the technical detail is agreed and it can be pretty tedious for people to listen to.

Dr Jan Collie: I am finding that we are getting more and more directions for experts to agree what they are going to agree on, and to agree what they are going to disagree about before it gets to trial, which of course is very sensible if it can happen. Sometimes it cannot happen because you cannot agree with each other, so you both have to go in. Sometimes it all happens so quickly that the two reports go in and there is not even time for that. The judge will quite often send you out into a room to knock your heads together and will say, "Come out when you have agreed something and let us know the answer". That is all very sensible but it does not happen all the time, especially when things happen very quickly, as Peter was saying. Sometimes they will phone you up mid-trial and say, "Quick, quick, can you look at this? Quick, quick, can you give me an opinion on that? By the way, the judge wants it by Thursday", and this is Monday, and you throw your hands up in despair, because it cannot be done that fast, and it is not as if we do not have anything else to do.

Professor Peter Sommer: One of the areas where it is useful is where you need to explain a bit of technology—how something works. Every so often a prosecutor will come up with a diagram or even some moving video to try to make a point, and it is important that the defence gets to see that and says, "Yes, we agree", so when the evidence is presented to the jury, it can say, "Yes, this particular bit of explanation has been done". I am being asked to do something like that right now.

Q126 **Lord Renfrew of Kaimsthorn:** I am feeling rather disquieted. I am getting the impression from what the three of you are telling us that we have here a rather chaotic field. I was particularly surprised to learn that you would not be aware usually of what the judge had said in his summing up. I am therefore rather uncertain how you get an overview—I suppose as an expert witness it is not your job to get an overview—of what has happened in the trial and its result. I have a prepared question here: is enough being done to prepare for the increasing role that digital forensics will have in the future? I think what you have said already gives a negative answer to that, but what should be done in the system so that

the role of digital forensics is properly understood in the criminal justice system?

Mark Stokes: There are many factors in answering that question, but it certainly includes the presentation of the available knowledge and information in a dynamic manner so that it can be accessed by the whole of the judiciary, the CPS, and jurors even. It has to be validated and put there and managed in the right way so that it is correct. Googling it will not work at all.

There needs to be more investment and co-ordination in research and development. A lot of the things that we do are last minute. Some of them are impossible to do and some of them are possible to do. There is not enough knowledge and understanding of where those limitations sit and of the timescales and the complexity of what you may be asked to do. It might be an application or something that you have never seen before that needs to be reverse engineered. It may be possible to reverse engineer it or it may take you a long time to reverse engineer it. There has to be a complex conversation about that. Going full circle, within the criminal justice system those conversations should be happening about the points to prove within the investigation and what the defence case is. The defence case should be clearly stated early on in the trial. That does not always happen. In fact, that happens quite infrequently.

Dr Jan Collie: I have to agree with that.

Lord Renfrew of Kaimsthorn: Why does it not happen in the trial that the defence case is stated? Could you clarify what you just said?

Mark Stokes: There should be a clear defence statement in that trial. It is very rare that we get a defence statement even fed down to us within digital forensics within policing, and, if we get one, the clarity of that defence statement may be poor.

Lord Renfrew of Kaimsthorn: You are saying that the defence statement would be in advance of the trial?

Mark Stokes: Yes.

Professor Peter Sommer: It is part of the Criminal Procedure and Investigations Act that you have to produce a defence case statement.

Mark Stokes: What it is that the defence is saying against the prosecution's case and evidence, and I am talking about within a digital context here.

Dr Jan Collie: To be fair, and I am probably going to lose some friends by saying this, I find that quite a lot of defence lawyers are not that organised when it comes down to it and they frequently do not think about the potential value that the digital evidence might have in a particular case. Therefore, they are racing to the finish and they think about it a couple of weeks before the trial. It is too late because you cannot get access to it that quickly. Even if the officer in charge of the case knows where it is, it is highly unlikely that he will get hold of it within a couple of weeks. There is quite a lot of disorganisation there.

Mark Stokes: As forensic practitioners working within the prosecution context, we are still independent professional practitioners, and we are there to help both sides. If we know both sides of the story, we can help to unravel whatever it might be, for example in a complex rape case the data and messaging. We have had cases with 44,000 social media messages on one device. If you have the defence saying one thing, or not saying anything, and the prosecution saying something else, you need clear guidance on what that defence is going to be and what to assist with.

Dr Jan Collie: We also need to work together more effectively because it is not always the case that the prosecution is sitting there waiting to be my friend. Frequently, that is not the case.

Professor Peter Sommer: In an earlier session, witnesses drew a distinction between what they called the luxury end and the routine end. It is certainly my experience, and, as I have been around rather a long time I tend to get the luxury cases, that the luxury cases tend to be done rather well, because people are determined to do things properly and you get the very best people. The concern at an anecdotal level, and you are hearing it from Jan now, is below the luxury level, and that is where the problem lies.

Lord Borwick: To follow up on Lord Renfrew, we have received evidence that about 70% of crimes have a digital element.

Dr Jan Collie: It is more than that.

Lord Borwick: How many trials have a digital aspect to the evidence? How often is digital evidence brought out in a trial? Does that difference between the two percentages imply the amount of growth that should occur?

Professor Peter Sommer: Unless Mark knows differently, I do not think the statistics are being collected. To give you an example, I was instructed in a particularly gruesome murder case, and the digital evidence was that the accused said he was not there at the place of the murder, and he could prove it because there were computer logs on another computer in another location. It was a tiny part of the overall case. I do not think anybody would be collecting those statistics, but it is to illustrate that it is all pervasive. I do not know where the 70% figure comes from. It might be 90%.

Mark Stokes: In terms of investigations across all types of crime, we believe—and it is anecdotal I am afraid, and we do not have clear statistics—it is nearer to 90% of crime that has a digital element, in the broadest sense of that: CCTV, communications data, social media data, cyberattacks.

Lord Borwick: What percentage of trials brings out that evidence?

Mark Stokes: We do not know.

Lord Borwick: Is it your experience that most trials have digital evidence or a small minority of trials?

Professor Peter Sommer: The only trials I know where there is digital evidence are where they ring me up.

Mark Stokes: We are only involved in the ones that have digital evidence. I would conclude, even if there is a bit of attrition in there, that you are talking about a large number of criminal trials, which is all I can talk about, and obviously most fraud cases will be digital these days. Probably about 90% of murders and complex rape cases will have a digital element in them.

Q127 **Lord Mair:** In the context of digital forensics, it is clear that the data that you are dealing with is increasing all the time. Can you say something about the role of machine learning?

Professor Peter Sommer: I do not know whether you have had it yet but I was a bit disturbed by some of the things that were being said in earlier sessions and I have sent in a briefing note. Have you had that?

Lord Mair: We have seen that, thank you.

Professor Peter Sommer: The first thing to say is that people use this phrase "artificial intelligence" much too loosely. The definition keeps on changing. That is why one prefers to talk about machine learning because it is rather more specific. We use a lot of computer-searching techniques and computer-analysis techniques. I am not sure that machine learning in the criminal system is particularly beneficial. It works very well in civil e-disclosure, where you can get agreement, and there is a need to use a technology-aided review to plough through lots and lots of documents to see whether they are relevant. You do that by giving the machine-learning program a sample to work with, to enable it to devise some rules and to follow them. It does not work in the criminal system.

In terms of the various technology techniques that are available, Mark has already hinted at the fact that the real difficulty is looking through chat logs and social media messages where the language is highly informal and a lot of slang is used, and the only way to do it is to go through it with an interpretation which you then show to the other side and see whether they will accept it.

Lord Mair: I understand exactly your point about machine learning. Are there any advanced technological methods that you are using to be able to deal with all this data?

Mark Stokes: I would slightly disagree and I would like to turn this round the other way, if I may. If you imagine a modern mobile phone today, it could have 1 terabyte of data on it, which is 78 million documents or pages of information on one mobile device, and it is becoming impossible for an investigator to review, disclose, analyse, view and read all that information. Therefore, artificial intelligence and machine learning both have a part to play in this, but we have to be very careful in the application of these technologies. We need academia and science to work with us to do the testing and validation. These systems learn—there is a clue in the name—from how they are taught, and if the wrong people teach them they will learn the wrong things, so they could

bias themselves in one direction or another. They absolutely have a part to play. Large-scale computing and data storage systems have a part to play. I come back to the fundamental challenge: it requires investment and money because huge amounts of data need processing.

Lord Mair: They have a part to play, as you say, but the real question is: how much are they playing a role now, or are you talking about the potential?

Mark Stokes: It is in its infancy. Some of it is being applied, but we still need to do a lot more work to understand how those systems are working. Are they missing data? Do they produce false negatives? There is a whole lot of science that needs to go behind that. Again, it is a problem within digital forensics and forensic science that we do not have that co-ordinated research and development, so you can have one force applying something and one force saying, "I am not going to do it", a private company applying something and another one not. It is very disorganised and not done together in terms of that validation and testing and ensuring that that software is giving us the right answer.

Lord Mair: Does that mean that at present it is still people who are having to plough through all this data?

Mark Stokes: Yes, for the majority. In the Metropolitan Police Service we are about to implement over the next 12 to 18 months some very basic search and review tools for officers. Again, it is the investment in the storage, the computing power and processing all that data which takes a long time.

Lord Mair: Dr Collie, what is your view?

Dr Jan Collie: I would echo what Mark is saying. It does not come into private practice a great deal because obviously the volumes of data are not as large as those the Metropolitan Police have to deal with. The main controversy is that human biases might be replicated by some of these machine-learning systems, and that has to be watched very closely, particularly in systems such as face recognition where race might be a variable. It has to be watched, and I am sure you are completely aware of that, and used with caution. Also, with artificial intelligence, it is very hard to explain what happened and how the machine came up with a particular answer. As a science, it is difficult to put your finger on it and say, "How did the machine come up with an answer?" I did some AI programing and sometimes you have to say, "I don't know. I put in that it and it came out with that".

Mark Stokes: You have to do the ground truth data experiments and produce the ground truth data. Again, we do not have a co-ordinated approach in the UK or England and Wales to do that. In the States we have NIST—the National Institute of Standards and Technology—that produce datasets and assist. Again, different forces and organisations are producing different datasets to test these systems. There is not a coherent co-ordinated approach to that research and development.

Lord Thomas of Cwmgiedd: You will not be able to answer this question now, but, first, could you let us have some figures as to the

amount of time the Metropolitan Police spends going through these documents and, secondly, on your investment programme, so one can analyse whether the investment is right.

Mark Stokes: The investment is not right. I can tell you that.

Lord Thomas of Cwmgiedd: We would like to see the figures and look at it. I said you would not be able to answer it now.

Mark Stokes: I can give you a ratio example. At the Metropolitan Police we spend circa £60 million on traditional forensic science and we spend £11.2 million on digital forensic science. In terms of the time police officers spend, I have one example, because I was at the thick end of it until midnight one night, trying to assist and trying to get some rationale from the judge. The judge insisted on a Friday night, at close of play, that an iPad was downloaded. It was a weekend's work. We eventually managed to get into the iPad, which was password protected, and recovered the data. It took 20 police officers all weekend to go through the data on that device.

Lord Thomas of Cwmgiedd: It would be useful to have the comprehensive figures.

Mark Stokes: I am not sure the Met Police can come up with figures of how long officers spend on this.

Lord Thomas of Cwmgiedd: As best you can because the investment is obviously very important.

Mark Stokes: We can try to do something.

Professor Peter Sommer: We ought to ask the National Crime Agency to examine it because it will have even more complex cases than the Met routinely have.

The Chairman: If you have real information, please send it. Can I move on to Baroness Young, please?

Q128 **Baroness Young of Old Scone:** You have mentioned the whole question of accreditation and the two ISOs. Is that the right mechanism for maintaining quality in the system?

Mark Stokes: My personal opinion is yes. I have to declare that I am also the chair of the Regulator's specialist group. I have listened to a number of people over the years talk about the different standards that could be applied. There are all sorts of standards out there for security and other aspects. The basic principles of ISO 17025 and 17020 are good and firm. They are about validating and testing software and systems and processes, understanding your methods and having an overall quality management system in place for your organisation. They are about understanding error, and ensuring that when errors occur, they are reported and fixed. They ensure that your staff are competent to undertake the tasks that they are doing and that they understand the complexities of the data they are processing or interpreting. They involve auditing—what we call proficiency tests, where blind tests are sent to laboratories and an expert will go through a test, where someone else

knows, independently, what the result of that test is, and they will check whether you have performed within that proficiency test. My personal opinion is that it is as good a set of standards as anything else that is out there.

Professor Peter Sommer: The limitation is this: ISO 17025 started out as a laboratory calibration standard and has been adapted and extended. It works pretty well for a lot of traditional trace forensics where you want to run a particular test and for that test to be properly designed and executed and so on. That was very much the view you were getting from the forensic science society witness earlier this afternoon. The problem is that the tools that of necessity we use contain lots and lots of bits of different knowledge. I do not know whether you have had it demonstrated to you, but the way most of these tools work is that you are presented with a total view of the contents of a computer or a smartphone and within that, as a result of lots of reverse engineering, individual tests, which have never by themselves been tested out, are displayed. You have to make a guess as to whether you are going to accept it. You can never have a proper accreditation of the sorts of tools the vast majority of people use. That is the point that I think Angus Marshall was trying to make in the previous session. I know Mark disagrees with me.

Mark Stokes: I fundamentally disagree.

Professor Peter Sommer: Which will make it interesting for you.

Dr Jan Collie: I happen to agree with Professor Sommer on this.

Mark Stokes: All systems will have errors in them. We will never understand everything that is going on within complex systems. It is to do with programing and is very complex. If we know nothing about those systems that is even worse.

Dr Jan Collie: It is not a case of knowing nothing about systems; it is whether that test is appropriate. Most of the forensic tools we use are tested to within an inch of their lives by the companies who produce those tools. We are not allowed to reverse engineer them because that would be illegal anyway.

Mark Stokes: That is not strictly true.

Baroness Young of Old Scone: Let me try to unravel it for the benefit of lay readers, if I can put it like that.

The Chairman: Mr Stokes, you finish first what you were saying.

Mark Stokes: At the end of the day, it comes back to what I was talking about earlier. It is ground truth data. It is very difficult and complicated and not like traditional forensic science. That is why some of the Regulator's timescales are challenging because it takes time to develop those datasets that represent what someone would do on their device, so you know what data you are putting into the system and can work through as an expert what you expect to come out the other end and the errors there might be within that system. Take, for example, times and dates, there are classical things within digital forensics that can get

misrepresented. You would make sure that you put in representative data that has times and dates that you know, and you see what the system does, and whether it reports those times and dates correctly. That is just one example.

Dr Jan Collie: Would you do that for every update of Windows 10?

The Chairman: One at a time, please.

Mark Stokes: It is the testing and validation of the method. You do not do it for every variable. It is academics talking now and we will have an argument among ourselves, if we are not careful.

Dr Jan Collie: I am not an academic; I am a practitioner.

Mark Stokes: Within the validation of a method, you do not use every aspect of a tool, so you can focus down on the process and method that you are testing and validating, and ensure the person acting upon and using these tools and undertaking that method is competent to do so. That is the scope of the validation.

Professor Peter Sommer: The other mechanism that is available is in the courts. If you go back to the Criminal Procedure Rules and how they cover expert evidence, and forensic science as a subset of it, there is an opportunity to check, and that is where the role of the defence expert is so key. The products that are used to perform the original analysis on the prosecution side are always going to be defective. If a defendant raises with his or her solicitor that they are dissatisfied with the results, the solicitor will call in an expert who will track through all the work. If the work has been properly documented according to the requirements of the Criminal Procedure Rules—and they lay down extensive lists of requirements of what ought to go in—the defence experts provide a backstop and reassurance that something is worthwhile. The idea that you can accredit any of these tools is, I am afraid—sorry, Mark—delusional.

Mark Stokes: You are not accrediting the tool; you are accrediting the methodology and the process. It is very different.

Dr Jan Collie: I want to throw the cat among the pigeons here slightly because I do not think the same tests that apply to DNA forensics apply to digital forensics. It is a different kettle of fish. How can you recover stuff that is out on the cloud in a forensically sound way? How can you prove you have done it in a forensically sound way? The other thing is cost. I heard some of the other witnesses speaking earlier. The costs of complying with some of these standards are going to be absolutely phenomenal. Not only will it put some people out of business, a lot of police forces cannot afford it. What is going to happen is that police evidence could be rendered inadmissible if certain forces have not managed to achieve the standard in time. That is going to be quite big.

Mark Stokes: I do not think it will be inadmissible. There are several things in there. First, if something is produced in error or by mistake, the criminal justice system, including the practitioners from both the prosecution and defence, has a role in there to identify that. Everyone in

that system has a role to identify that. At the moment we do very little testing and validation, and people are already using these tools, so anything is better than what has happened before.

The Chairman: We have got the message. The message for our report is that you guys need to get to a position where you can all agree.

Dr Jan Collie: I think it is going to be a very long time before we all agree on that.

The Chairman: That is not going to help the criminal justice system.

Dr Jan Collie: I am sorry it is bad news, but there have not been really good anonymous polls of everybody in the industry. I own my own company so I can say what I like. A lot of people think very similar things to that which I think about the criminal justice system and these ISO standards, and they dare not say anything because it is their boss's company.

Mark Stokes: I agree with a point you made; it is complicated. There is not enough funding within the system to do it within the timescale.

The Chairman: Can I stop you, please? Lord Griffiths.

Q129 **Lord Griffiths of Fforestfach:** What statutory powers do you think the Regulator should have? If the Regulator is given those powers, what different outcomes should we expect?

Professor Peter Sommer: It depends entirely on the remit. If she sticks with her current remit and wants to force ISO 17025 into situations where it does not work, it will be a disaster. It is expensive for the police, as you have heard Jan say. In effect, external experts kick up a fuss but then say, "I can do digital forensics and there are 50,000 fewer cybersecurity experts than we need; I will go off and do that and earn three or four times as much", and that is what is happening.

Lord Griffiths of Fforestfach: Do you think the Regulator should be given statutory powers?

Mark Stokes: Yes.

Professor Peter Sommer: Not at the moment.

Lord Griffiths of Fforestfach: You think not, you think yes; what do you think, Dr Collie?

Dr Jan Collie: I would approach that with great caution and I would want to have some idea of what that might mean, to be absolutely honest.

Lord Griffiths of Fforestfach: Could I ask the Metropolitan Police for its view?

Mark Stokes: It is necessary in forensic science, the medical profession or anywhere else where experts and people are doing things that are really important. What those exact statutory powers should be is up for some real discussion.

Lord Griffiths of Fforestfach: Are there some statutory powers that

you can all agree on that should be given to the Regulator?

Mark Stokes: An expert could be suspended if they are not acting appropriately. I think that is a power that should be there.

Professor Peter Sommer: There is an inquiry role that I would certainly endorse, but at the moment the Forensic Science Regulator thinks that one model, the model that works for trace forensics, can be forced on to situations where it does not work, and it is important to go back and have a look at what expert testimony is in addition to forensic science. It would have to fit into that framework, I do not think she has ever understood it because she comes from a DNA background and nearly all the advisers tend to come from a trace forensics background as well. As you have heard, digital forensics is very different. It can still be scientifically and carefully explained.

Lord Griffiths of Fforestfach: Can I ask a question on an area I know a little about: the Financial Regulator? When it comes to how much capital banks should have, there is no question that it is their judgment, they have a reason for doing it, and it is accepted by the industry. When it comes to them saying what the culture of an institution should be, they may be able to determine some elements of what it should include, but they would not determine it in the way they would determine, for example, capital. Are there not some things in your business which are the equivalent of capital requirements on banks where you can all agree and say, whoever is in this whole business of forensic science, there should be certain standards which have to be met for competence to practise?

Professor Peter Sommer: I am not sure that parallel works. The other area you can look at is certifying individuals.

Mark Stokes: Qualifications are not per se an indication of competence.

Dr Jan Collie: I was about to say that we do not have just qualifications but organisations such as the British Computer Society and the Institute of Engineering and Technology—IET—and to gain competency in those you have to jump through quite a lot of hoops. These things exist.

Mark Stokes: I would slightly disagree. This is different.

Lord Griffiths of Fforestfach: Mr Stokes, do you think there are statutory powers that could be introduced which might improve this field?

Mark Stokes: Just because someone has a degree in electronic engineering or computer software programing does not per se make them competent to be a digital forensics practitioner or a forensic scientist. The training and competencies and interpretation are entirely different. The qualifications are a foundation stone and a basis; they are not the competence to carry out the activity.

Dr Jan Collie: Where does that leave an officer on the street in all this?

Mark Stokes: I could not comment. I am not a police officer. I am not here to talk about the police.

Baroness Neville-Jones: On this question of whether the Regulator

should have statutory powers, I am not at all clear whether you are saying that there are no circumstances in which that is going to be appropriate.

The Chairman: Yes or no?

Baroness Neville-Jones: Or are you saying, "The way the role is being conducted at the moment is not one I would like to endorse and therefore I have real reservations about it"?

Professor Peter Sommer: Answer number two.

Baroness Neville-Jones: Is that answer number two?

Dr Jan Collie: Yes.

Mark Stokes: I have made my point very clear, I think.

Baroness Neville-Jones: Answer number one.

Mark Stokes: Statutory powers are required, although what those should include needs some discussion and thought.

Q130 **Lord Kakkar:** I want to turn to the question of the research base that supports the practice of digital forensic science. Is there a strong and robust research base? How is it conducted? Is there an opportunity for collaboration for those who have an academic interest in this area to further inform the development of this field?

Mark Stokes: No, no and not a lot, in that order. There is no co-ordination within digital forensics research and development. There is little input as to what projects or research should be undertaken. Again, I think the previous witnesses have said that fundamental science has a role to play here as well, but it is how you adopt that into forensic science disciplines. There is no co-ordination and a lack of funding. We have certainly struggled with getting funding from the EU and other places. We try to work closely with academia but, again, when your day job is trying to process 50,000 exhibits a year, there is not the bandwidth to undertake that as individual forces. That needs to be co-ordinated through something such as Transforming Forensics but being very focused on outcomes and developing that research and development.

Dr Jan Collie: Sharing research findings is often held back because people smell a saleable product and they do not want to share that information. I often see that, to be honest.

Mark Stokes: That is a point but fundamental research should be peer reviewed and published within digital forensics.

Lord Kakkar: But it does not happen in digital forensics.

Mark Stokes: People are not doing it.

Professor Peter Sommer: We also need artefact research. Earlier on I was saying that the tools that people use contain hundreds, maybe even thousands, of different bits of knowledge. People have had to reverse engineer new products or new versions of products as they come out to see how they work, and a lot of this is never written up. What I have

tried do is encourage undergraduates and master's students to try to do this sort of work because it makes rather a good way of measuring whether someone should be getting a particular sort of degree. I agree with Mark that there is no central resource where one can go along and say, "Which are the bits that I need to be looking at?" At the moment you are getting lots of people looking at IoT devices because they are the new thing. You get quite a lot of people looking at cryptocurrencies and probably duplicating themselves and other stuff that is not being looked at at all.

Lord Kakkar: If people are not looking at the broad base of the science that underpins digital forensics, how confident can we be that the methodologies and tools that are being used are reliable?

Professor Peter Sommer: The underlying methodology is perfectly straightforward. You carry out an observation; you form a hypothesis of what might be happening; you devise a way of testing it; you carry out the tests. Having carried out the tests you look at the results. If you need to modify your original hypothesis, you do so. You publish it and put it up for peer review. It is exactly the same.

Lord Kakkar: Does that happen for the broad base of digital forensics?

Dr Jan Collie: I think it happens more in America than it does here.

Mark Stokes: Outside the UK in Europe and America, absolutely. In the UK, it is very fragmented and there is not so much work going on in academia, certainly not within digital forensics laboratories where people have time to do research—

Professor Peter Sommer: Specialist journals exist—

The Chairman: Professor Sommer, could you allow Mr Stokes to finish, please?

Mark Stokes: The challenge is that research and development and peer-reviewed publications need to come jointly from academia and digital forensics labs and from within digital forensics labs. The bit that is missing is the guidance from the front of the business as to what research we need to focus on, and having the capacity within a digital forensics lab to work with academia in the UK to produce that research work and that ground truth data and that understanding of tools, techniques and interpretation.

Lord Kakkar: How can that be made to happen? Is it important that it happens in the UK, or are you content that it happens elsewhere in the world?

Mark Stokes: We were leaders at one time, certainly within traditional forensic science, and we started to lead in digital forensic science at one point. Digital forensic science across the world has grown up slightly differently from traditional forensic science. To answer your question directly, it needs more funding and it needs central co-ordination. I do not have the answers to either of those as I sit here.

Dr Jan Collie: There needs to be more opportunity to publish as well, because what tends to happen is that these academic journals turn into a bit of a club.

The Chairman: Is there a journal of forensic science?

Dr Jan Collie: There are lots of journals on various aspects of forensic science.

Professor Peter Sommer: I am on the board of two of them.

The Chairman: I have the answer. This last question is important and we need each of you to give an answer. Baroness Neville-Jones.

Q131 **Baroness Neville-Jones:** That is precisely my approach, Chairman. It seems to me that there is quite a lot disagreement among the witnesses and so you may have different answers to this question. If you had to make one recommendation, in what seems to me in many respects to be a rather unsatisfactory situation, which would have great impact in improving the quality of forensic science and its ability to contribute to the delivery of justice, what would it be?

Mark Stokes: Just one. More funding.

Baroness Neville-Jones: Life is a matter of priorities, so which is the one?

Mark Stokes: Funding. It needs more funding.

The Chairman: Funding for what?

Mark Stokes: Across the board: for research and development, co-ordination, training, including for the judiciary where they could have access to knowledge and information, as we have described. All those things need funding and putting in place and need the people behind them.

Baroness Neville-Jones: Where would you start in your funding? Where would you want to put the money first?

Mark Stokes: At the moment in digital forensics within England and Wales, the capacity to undertake what is required on criminal investigations is not there. We currently have a seven-month backlog. We are reducing some of that backlog by outsourcing, but I described the mobile phone with 1 terabyte of data, and there are huge amounts of data, and you need to invest in the capacity and training to meet the demand. We cannot meet the demand currently with what we have.

Dr Jan Collie: I would go back to what we were saying about training. If the system is going to be that ordinary police officers are being asked to download information off digital equipment, they ought to know at least how to do it in a way that is not going to foul the evidence or put them in a difficult situation when they have to go to court. Anybody trying to interpret what comes out of these things should know how to interpret it and it should not be put on to the shoulders of people who cannot possibly have had the right amount of training to do that.

Professor Peter Sommer: I do not disagree with either of those things, but I would like to raise a separate issue. It seems to me that a lot of Home Office policy and forensic science regulation policy has gone on the basis of rather vague anecdotes. Your specialist adviser and her colleagues did a rather interesting examination—

The Chairman: You are making a recommendation; what would it be?

Professor Peter Sommer: It is a recommendation. The recommendation is to research where things are going wrong with forensic science rather than just saying that it is a scientific problem within labs which can be solved with ISO 17025. You need to look at the whole range and decide whether things are going wrong at the specification level, at the investigator level or at the disclosure level. A little bit of research has been done, but not very much. We need to do more, otherwise we do not know how to spend our money.

The Chairman: Lord Mair, did you have a burning question?

Lord Mair: No, I do not.

The Chairman: I ignored you earlier on and I am sorry about that. We have gone on a bit longer than planned, but thank you very much. It is has been an interesting and heated discussion. You might go into a corner somewhere now and see what you can agree on. Thank you very much for coming today; it is much appreciated.