Fraud Act 2006 and Digital Fraud Select Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 9 June 2022

9.35 am

Watch the meeting

Members present: Baroness Morgan of Cotes (The Chair); Baroness Bowles of Berkhamsted; Lord Browne of Ladyton; Viscount Colville of Culross; Baroness Kingsmill; Lord Sandhurst; Baroness Taylor of Bolton; Lord Vaux of Harrowden; Lord Young of Cookham.

Evidence Session No. 19 Heard in Public Questions 197 - 211

Examination of witnesses

Mark Fenhalls, Karl Laird.

The Chair: Good morning and welcome to this evidence session of the Fraud Act 2006 and Digital Fraud Committee. A transcript of the meeting will be taken and published on the committee's website, and you will have the opportunity to make corrections to it where necessary. We are delighted this morning to be joined by Mark Fenhalls QC, who is chair of the Bar council, and Karl Laird, who is a senior lecturer and tutor in law from Oxford University. Without further ado, Lord Young will ask the first question.

Q197 **Lord Young of Cookham:** Good morning. To set the scene for an overall general question, the objectives of the Fraud Act 2006 were to make the law easier for jurors to understand, to allow for effective prosecution, to be fair to potential defendants, and to meet the needs of developing technology. What is your overall assessment of the Fraud Act 2006 in meeting those objectives?

Mark Fenhalls: My assessment is that it has achieved its objectives. We have seen this morning in the document supplied that the 2012 review broadly said that. All the barristers I have spoken to since being invited to give evidence cannot think of a particular example of where something has gone wrong or the Fraud Act has made it harder. On the contrary, the removal of the operative deceptions made life easier. The problems that arise in prosecutions of these kinds of offences are all practical ones. They are not around the conceptual framework. That is the broad feeling.

Lord Young of Cookham: Karl, what is your assessment?

Karl Laird: I would agree with that. There are four factors that explain why the Fraud Act has been a successful piece of legislation and has achieved the aims it was set out to achieve. The first is that the offences are conduct crimes, so they do not require the prosecution to prove any particular result. Secondly, the offences are exceptionally broad. Thirdly, the Fraud Act is a short piece of legislation that is unburdened by the technicality that undermines the effectiveness of the legislation that it replaced.

Fourthly, it was intended to be futureproofed. To give you an example, one of the issues that bedevilled the old law was the inability to deceive a machine, because under the old law it was required for there to be a deception, and machines cannot be deceived. That was obviously a significant impediment to the deception offences being used in the electronic age. That requirement of deception was removed in the Fraud Act specifically in order for legislation for the offences to be capable of being used in the electronic age.

Lord Young of Cookham: That is very helpful. So despite the changes in technology and the changes in the types of fraud, your view is that the Act is still fit for purpose.

Karl Laird: Yes.

Mark Fenhalls: Yes.

The Chair: That is very clear. Thank you very much. For the benefit of those watching, the document that we are referring to is a memo, published by the Ministry of Justice this morning, on the Fraud Act 2006.

Q198 **Lord Vaux of Harrowden:** You have touched on this question already, but obviously in the last 15 or 16 years since the Fraud Act came into power, technology has moved on quite significantly with cybercrime, crypto et cetera. Does the Fraud Act cover those adequately, and can other changes be made to it to make it better in respect of covering those areas?

Karl Laird: When the Fraud Act was drafted, it was drafted with these issues in mind. Obviously the draftspersons could not have had in mind the specifics—bitcoin, for example. However, they very much had in mind that the legislation, the offences, would need to be capable of keeping pace with technological developments. One way in which the Act achieves that is the definition of property. How we conceptualise property has changed in a number of respects, even in the past 15 years. The Act accommodates that by not having a very prescriptive definition of property, but a very broad definition of property that is capable of encompassing things that are tangible but is also capable of encompassing things that are intangible, such as blockchain. That is one example of how the legislation was drafted with a view to it being capable of prosecuting it in the future with a view to it not becoming quickly out of date.

Lord Vaux of Harrowden: We have seen some evidence. The City of London Police, for example, have indicated that they have felt that there are deficiencies. Is that more down to a misunderstanding of the way the Act works, or are there other areas?

Karl Laird: Deficiencies in what sense? Do you mean that the Act is too narrow or that there are difficulties with enforcement, with prosecuting, with investigating these offences?

Lord Vaux of Harrowden: I do not have the full evidence in front of me, but further offences could be added that suit more complex digital cases of online fraud. The Nottingham Building Society has told us that there have not been enough amendments to keep up with changes for providing adequate coverage of crypto assets. That is not terribly specific, I confess, but your view would be that you disagree with that and that it should cover it?

Karl Laird: Yes, and frankly it is difficult to envisage how the offences could be drafted any more broadly. They are offences of exceptional breadth. They are some of the broadest offences that exist in English criminal law. If they are incapable of encompassing these forms of conduct, I would struggle to see how any offence could encompass the conduct, given the difficulty in seeing how an offence could be drafted any more broadly.

Lord Vaux of Harrowden: Thank you. Mark, do you have anything to add?

Mark Fenhalls: I agree with what has been said. I would probe very carefully anybody who says that there are deficiencies or that improvements could be made. Quite often, people say that because it is an excuse for them not having acted in a particular situation. I am not aware of any evidence that there are such deficiencies. All the practical examples I have had on and off over the last 15 years have revolved around challenges in identifying new tech and finding out what it is.

Back at the end of the noughties, a group of police officers walked into a house, seized all the electronic equipment there, and happened to seize an iPod. They had no idea that it was a hard drive; they happened by chance to search it. All the identity documents that had been used in this massive car rigging case were on this iPod and there was nothing on any of the computers. Once they had found them, there was a cast-iron case. I think it made the front page of Apple News, because it was the first time that this had come up.

That is not a bad illustration of how the challenges are all technical. It is the police having the training and the resources to keep up with the changes, rather than deficiencies over the law.

The Chair: That is very helpful.

Q199 **Lord Browne of Ladyton:** Good morning, gentlemen. My expectation is that the subject of this question is the meat of this session. I could

probably summarise it quite easily by saying, "If it's not the Fraud Act, what is it?", because there is a problem. The number of frauds has expanded exponentially. Prosecutions are minimal compared to that number, and convictions even more so; they are virtually non-existent. What is the problem? What are the barriers? We will probably spend some time exploring these, and you have already suggested some of them. What are the barriers to a successful, swift prosecution that reflects the importance of these issues?

Mark Fenhalls: I should preface my remarks by saying that I have spent a lot of time prosecuting and defending fraud in the last 15 or 20 years. It has been a particular concern of mine to see the collapse of fraud investigation as a political decision. I think the state has retreated from the investigation and prosecution of fraud over the last 15 years, and I am afraid it is a consequence of political decisions about resources, and priorities for police forces are set, ultimately, by politicians and those who allocate resources. I am afraid that is the blunt reality.

I remember 10 years or so ago prosecuting an enormous case in Norfolk, its biggest ever fraud case, and dealing with an outstanding detective constable, who was the last member of its fraud squad. That is the reality; as political changes have taken place, we have moved from having expert police officers dealing with this, because the priorities lie elsewhere. I am not blaming politicians for the competition and challenges of resourcing, because, of course, we know what the other competing demands are. However, the reality is that Action Fraud as a concept, as a website, acts more as a way of stopping the investigation and prosecution of fraud than anything else.

It would be worth you going back to the *Times* exposé of August 2019 when it sent in reporters who then worked for Action Fraud, because after that front-page story it was the first time ever that officials and politicians began to even listen to me. I have been complaining about what had been going on for the last decade. Nobody wants to deal with the elephant in the room, which is that you cannot do anything about this unless you resource the police properly and give them a chance to investigate. That exposé made a significant difference to the debate. It meant that people accepted that there was a real problem. In Action Fraud, people were saying, "Let's try to filter out as much as this as possible. We want to avoid as many of these cases as possible. They're tricky, they're difficult, there are all kinds of barriers later on and we do not have the resources to deal with it". There are all those sorts of practical issues around it.

Many people will contact you, and certainly constituency MPs, saying, "I've been the victim of fraud. Who do I contact?" I get many a year. They say, "I've tried Action Fraud. I can't get through to it. You can't find a police officer to speak to to do it". There is a structural problem here, which the Home Office has to tackle if we, as a society, are to make a significant difference. I have gone on for far too long on that.

Lord Vaux of Harrowden: It is a very good start, though.

Mark Fenhalls: You can tell that it is one of my hobby horses.

Lord Vaux of Harrowden: We like hobby horses.

Karl Laird: I also wonder if fraud is an underreported crime. In contrast to other acquisitive offences such as theft, I wonder whether people who find themselves victims of fraud are reluctant to seek help, because they feel as though they have been swindled and are almost the author of their own misfortune. I wonder whether there needs to be greater awareness that anyone can be a victim of fraud, especially in the modern era, given the lengths to which fraudsters will go commit their offences. Of course, given that we all have electronic devices, that makes it somewhat easier today to commit fraud than it would have been in 2006 and for fraud to reach a much broader range of people.

Lord Browne of Ladyton: The evidence that we have received suggests that it probably is underreported, but, then, almost all crime is underreported unless it is created by an interaction between a police officer and somebody, like drunk driving or something.

It is improbable that our recommendation will be that we just scale everything up, because that is not likely in the current financial environment; we all know that response. The question is what we can do about some of these issues that people have spoken to us about. Let us take GDPR, for example. People tell us that that causes problems with sharing information and the way in which we can investigate. We are pretty sceptical about it, I would say, but it would help us if we had the opinion of a QC that we were right to be.

Mark Fenhalls: I am curious as to how you are sceptical. Can I give you a practical example? Over the last few months I have completed a substantial-scale pension fraud. I will not talk about it very much, because it is due for sentence in a month's time. It was much delayed by Covid and quite challenging. The jury was sensational in the way it kept going; all parties were. However, the police team in that case were paralysed by the demands of editing the documents. There is a vast quantity of material in certain kinds of fraud that contains personal data—in this case, of people who had been customers of this business. The requirements of the current system meant that the Crown Prosecution Service and the police felt obliged to put in thousands of man-hours editing out personal details from all these documents.

The Chair: Before they could be shared with the court and the jury.

Mark Fenhalls: Yes. That is a spectacular burden. It is undoubtedly the case that the Information Commissioner's Office is extremely zealous about these matters and will spend its life fining the CPS if these things fail according to its terms. Dealing with the question of personal data is a huge practical problem for society. I will deliberately steer away from the question of people's phones and all the issues around serious sexual offences, which are a subset of critical importance, which in a sense the state is looking at separately.

However, if you have a case where the defendants have all been in possession of this material in any event in the past, there ought to be a way to say, quite straightforwardly, that this is covered at the moment. I think there is; it is in Section 17 of the Criminal Procedure and Investigations Act in the way in which it is policed, because you are given this material for the purposes of that case only.

If that was enforced and used, and we could just recalibrate the Information Commissioner's approach a little bit so that there was something fashioned around at least a criminal justice understanding, if not exemption, that in the context of a criminal case we could decide that it is covered in this way and that everything is fine in this case, that the section in the Criminal Procedure and Investigations Act and the contempt that you will be liable to if you use it or misuse it will apply and bite, then there is a way, with enough wit, in which those thousands of man-hours can be saved.

Lord Browne of Ladyton: Can I test this a bit? I accept from you, because you have experience of this that I do not have, that that is the way the system operates. However, the effect on me of all your evidence to us thus far is that the system is wrong, and that there is a way of doing this in the rules that could be adopted, but it is being presented to us as if these are the rules and we have no alternative. Is there actual experience of the Information Commissioner's Office actually pursuing people for breaches of that nature, or is it just feared?

Mark Fenhalls: It is a combination, but the CPS is fined frequently by the Information Commissioner's Office.

Lord Browne of Ladyton: Is that right?

Mark Fenhalls: I have CPS lawyers who say, "We have to do this; otherwise, we will get another fine".

Lord Browne of Ladyton: We will now hunt this data, because this is important, I think.

The Chair: Absolutely.

Mark Fenhalls: I would be thrilled if you would take it up.

The Chair: We have the Director of Public Prosecutions coming before us next week.

Lord Browne of Ladyton: I will retire from this.

The Chair: You have raised a forest of arms now.

Q200 **Viscount Colville of Culross:** That is very powerful evidence. What do we need to do with the GDPR? Do we need to change it, or just ask the commissioner to hold back on prosecuting the CPS for disclosing this personal information?

Mark Fenhalls: My personal, least intrusive, least bad solution would be to get an understanding between, effectively, the Home Office and the ICO that there needs to be a bit of, if not flexibility, then latitude and understanding about the way in which these guidelines are being rigorously applied. I am not quite sure what the right mechanics are to do that, because of the unintended consequences.

Personally, I would ask that nobody interfered with GDPR, because of a separate issue, which is the dangers of effective drift from compliance with a set of standards that are common with the European Union and are of huge benefit to this country because of the common standards. On a separate but related issue, I am deeply worried about accidental divergence and that people changing rules here will mean that we drift further apart and that the country suffers because we are not able to communicate with the European Union in the way we should. Unless we can maintain dialogue and understanding of the common rules—we can do it all our own way, as we must now, but in a way that works with European Union rules—there are real risks ahead for the country.

Viscount Colville of Culross: Are you asking the ICO to hold off fining the CPS?

Mark Fenhalls: I would like an exemption, in a sense, for criminal justice that says, "The Criminal Procedure and Investigations Act works. Police that properly. Leave that to work as it does", and an understanding that, in the criminal justice system, societies' demands that we actually handle the case and save scarce police resources triumph here.

Q201 **Lord Sandhurst:** Can I declare an interest straightaway? You would have known me at the Bar as Guy Mansfield QC. I practised at the Bar until I retired three years ago. I was chair of the Bar in 2005. We have never met, but I thought that it was important to put that on the record. I dealt with crime years ago and sat as a Recorder for quite a long time.

Listening to your evidence, it occurred to me that what is needed is what you are talking about: a formal protocol governing criminal fraud cases, signed up to by the CPS, by the SFO probably, if necessary, and by the Information Commissioner's Office. There might have to be new rules for the Crown Court—criminal procedure rules or special ones, I do not know. Possibly the quickest way forward, although I am always chary, would be a motivated working group comprised of representatives of the CPS, the ICO and a good criminal judge who would bring the three different interests together, because you have to ensure that it works in the courts and that both defence and prosecution have a fair crack. Does that seem a sensible way forward to try to bridge this? Otherwise, the CPS and the ICO will continue to bat away. They need to be brought together formally.

Mark Fenhalls: If I may say so, that sounds like a very sensible step to explore and to try. It is always possible that I am wrong and that my preconceptions about this and my experience are not universal. If I may say so, the earlier you give notice of a director who you would like to

cover this issue, the more he can get somebody to do active research for him to see what the extent of the problem is. It sounds like a great start to at least explore this and see if we can unlock something.

Lord Young of Cookham: You were very critical about the volume of resources. What about the way those resources are used, the structure in the police force, with concentration in the City of London and then hub and spoke going out, and the way central government responds with what has been referred to as the alphabet soup of organisations that try to liaise? Do you have any view on the structure as well as the resources of the response?

Mark Fenhalls: Yes. I am not sure that they are all evidence-based, in the sense that I have a complete grasp of the way the country entirely works, but it works on every kind of level. If you begin with the 40-odd police forces, the different systems they have, and the way they do not necessarily integrate and the way fraud moves around, there are potentially more challenges with fraud than with other criminal offences.

I do not have difficulty with a concentration of resources in the City of London and the Met, because that is where most of it goes on. The problem is the absence of resources elsewhere. If you are dealing with a small force somewhere that has a certain number of priorities and fewer resources, in truth I am not sure how people are even measuring this. It might be a fruitful line of inquiry to cause some thinking about measuring the problem that they do not know they have, as opposed to the one that is right in front of them: "This many people have been killed on our patch this year".

Lord Browne of Ladyton: I want to go back to the GDPR, and I hope we can get corroborating evidence from Karl on this. Your consent to the excellent leading question that was put to you by my colleague is helpful to us. Karl, do you have any view about that discussion?

Karl Laird: I agree with Mark. It sounds like a good start. Perhaps what is being lost sight of is that, as Mark has already pointed out, in criminal proceedings there is primary legislation backed up by a sanction that protects information that is disclosed for the purpose of criminal proceedings. That provision is not necessarily reflected in other areas, so I wonder whether the zealous pursuit of the CPS is perhaps a result of an underappreciation that here is a specific regime, backed up by the threat of contempt of court, that already protects information in the context of a criminal prosecution that does not necessarily exist elsewhere.

Lord Browne of Ladyton: That is a very helpful addendum, thank you.

Q202 **Viscount Colville of Culross:** I would like to move on now to the Computer Misuse Act. We have had evidence from cybersecurity professionals who say that when they are using cybersecurity programs to check computer security they are very exposed, and that currently the only protections in the Act beyond the use of a warrant are when they can get an explicit authorisation, which obviously is not that useful if you

are trying to check the programs. Do you think there needs to be a change of authorisation regime in the Act, Karl?

Karl Laird: The offences in the Computer Misuse Act are focused on unauthorised access and unauthorised acts. I struggle to see how those offences would impact cybersecurity professionals who are acting in the interests of their clients. Is the premise of this question whether some kind of public interest defence should be inserted into the Computer Misuse Act? I have to confess that I am rather sceptical of public interest defences generally. In English criminal law, they are very much the exception rather than the rule. The only statutory public interest defence that I can think of is the one contained in the Data Protection Act. Ordinarily, we rely on prosecutorial discretion, prosecutors exercising their judgment in a sensible way, to ensure that offences are not charged in inappropriate circumstances. I do not see why we cannot rely on prosecutorial discretion in this particular context.

I can see the justification for public interest defences where, for example, compliance with the United Kingdom's obligations under the European Convention on Human Rights might be an issue, but I do not see how that would be an issue here, so I do not see the legal impetus for a public interest defence in this particular context. I do not see why we cannot rely on prosecutorial discretion.

Viscount Colville of Culross: Mark, do you have anything to add?

Mark Fenhalls: Only a small amount, in the sense that if my computer has been hacked and I want an expert to look at it, I will authorise access. If there is a system-wide hack, whoever owns that system can authorise access. I would assume that in the vast majority of cases that would cover most cybersecurity professionals' operations. If there is a specific example of something more unusual about which I am not aware because they are doing perhaps preventive inquiries, I do not know, but it cannot be that complicated to get permission from the people who own the systems in order to do it. I would encourage you to find out the real extent of this supposed problem before making any particular recommendations.

Viscount Colville of Culross: Karl, you talk about dealing with the prosecution and asking them to hold off rather than trying to introduce a public interest section into this Act. How possible do you think that is to do?

Karl Laird: To introduce a defence?

Viscount Colville of Culross: No, sorry, to ask the prosecution services to hold off from prosecuting cybersecurity professionals who are testing the security of a computer without the explicit authorisation of the owner.

Karl Laird: I do not see how it would be any different from any other exercise of prosecutorial discretion. There is obviously a two-stage test: there is the evidential test and there is the public interest test. We rely on prosecutors to exercise judgment in other contexts when they are

deciding whether or not to charge. Considering the public interest, I do not see why it is any different in this context.

Viscount Colville of Culross: The Fraud Advisory Panel, in evidence to us, has said that the Act is wildly out of date. Do you think that there are other ways in which the Computer Misuse Act needs to be modernised to stop digital crime?

Mark Fenhalls: I do not know, is the short answer. People can say that very easily. I would quite like them to tell you how it is out of date and how there would be an improvement, before we worry too much about it. It strikes me that the language of the Act is fairly broad and that most of the problems will revolve around enforcement again.

Going back briefly to your question about whether there been any prosecutions of cybersecurity professionals for infringing the Act, I have to say that I have not heard of any. There may be, but again it would be worth perhaps identifying the number of examples of these things before getting too concerned about practical changes to what might be a very theoretical issue.

Viscount Colville of Culross: Karl, do you think that wider changes need to be made in the Act?

Karl Laird: The Act was originally enacted in 1990, and it has been amended on several occasions in an effort to keep pace with technological change. Rather than the Act requiring amendment to keep pace with technology, perhaps part of the problem—this may be an issue of enforcement as well—is that the Act has become extremely complex. When you constantly amend an Act, the offences become overly complex. That is true not just of this legislative context, but of amending legislation more generally. I wonder whether it is not so much a case of there being a lacuna in the legislation, but that because it has become so complex, because it has been amended on so many occasions, it has become rather unclear when the different offences apply and how they relate to one another.

Viscount Colville of Culross: Could you give us an example of the overcomplexity of this Act and the problems that causes?

Karl Laird: Given the nature of the issue, it is important that the legislation has a broad territorial scope, because obviously cybercrime transcends national boundaries and national jurisdictions. In order to understand the extent to which the offences in the Computer Misuse Act apply extraterritorially, it is necessary to wrap a cold tea towel around one's head and scrutinise the provisions very carefully. I am afraid that even if one were to do that, the extent to which the offences do apply extraterritorially may still not be evident. Amendments were made quite recently to increase the extraterritorial scope of the offences, but those provisions are still extremely complex. I cannot think of any instances of them being charged. I do wonder whether one reason for that is the complexity of the relevant provisions.

Viscount Colville of Culross: Is it worth looking at the Act again to see whether you can smooth out those amendments and make it much more useful and simple?

Karl Laird: I agree with Mark that this would obviously need to be evidence-based, but the Act has become extremely complex. I co-author a textbook, and I have to say that when it comes to updating the chapter on the Computer Misuse Act, we always leave that to last, which is obviously a completely false economy because it takes so long. I always groan when it comes time to amend that particular chapter, because frankly it is always very difficult.

Viscount Colville of Culross: That does not mean it should not be tried.

Karl Laird: Correct.

The Chair: A lot of us will have sympathy with that approach, Karl.

Q203 **Lord Sandhurst:** I have a short question about the business of the inhibition of genuine counter-fraud agents and whether they really are inhibited. In the context of assisted dying, not long ago the DPP—I think it was the DPP—issued guidance about when there will be prosecutions and when there are less likely to be prosecutions. Would something like that help? I am only flying a kite. I do not have a view.

Karl Laird: I do not see why not. There is guidance that applies to other circumstances that prosecutors must have regard to when they are making charging decisions. The most obvious one that comes to mind is journalists and ensuring the protection of freedom of speech. However, in the example that you give—the prosecutorial guidance that applies to assisted suicide—the catalyst for that guidance being promulgated was a House of Lords decision that it was to ensure compliance with the convention. There would not be the same convention issues in this context, I do not think, but that is not to say that such guidance would not be welcome.

Lord Sandhurst: It does not have to be under the convention. It can just be, "This is our approach".

Karl Laird: Yes.

Mark Fenhalls: My answer would be maybe, but I would quite like to know how many times CPS lawyers told their bosses, "I've considered that prosecuting that offence, but I haven't for the following reasons". It would be quite interesting for you to know how prevalent this really is.

Lord Sandhurst: Absolutely.

Q204 **Baroness Taylor of Bolton:** This is a pretty straightforward question. We have been told that the legal framework for prosecuting fraud is too complex and requires codification, that things are not brought together, that you have to deal with economic crime and cybercrime, and that it should all be in one code. Do you think that is practical or desirable? You

said that the basic 2006 Act is fit for purpose. We have looked at chinks and other issues that might be causing some of the problems that we are concerned with, but would simplification, codification, help in any way?

Mark Fenhalls: The short answer is that I do not know. The Law Commission might have an interesting view on it, having put together all the work that it did in relation to the Sentencing Code that was enacted in 2020. That worked well to simplify, at least putting it all in one place. Consistent with what I said to you earlier, I do not think there is a practical problem with the laws that apply when you get to court. We have all thought through what the conduct is, we have shaped the charges or the indictment around what has gone on, and in my experience juries understand all the issues that they are presented with. For me as a practitioner, the candid truth is that I am less interested in exercises like codification, because I know how it works. If there are others out there who can provide decent evidence that it is an impediment of some sort or another, I would not stand in their way, but personally I have not seen the need for it.

Karl Laird: I agree. Obviously the Fraud Act is not a codifying statute. However, in terms of fraud, it is a one-stop shop. I would urge the committee to have practical examples of how the Fraud Act causes problems. The Sentencing Act is a good example of codification that can be very effective. However, the note of caution I would urge is that codification works sometimes, but it does not necessarily work in others. It works for some areas of law, but not others. It works for sentencing, because that is very much a uniform area of law and it was possible to codify the law of sentencing. However, I question whether, practically speaking, it would be possible to codify this area of law given the rather diverse spectrum of content that these offences are intended to deal with.

Baroness Taylor of Bolton: In terms of what causes problems, is part of the difficulty we are facing that the cases, including the ones that Mark was talking about a few minutes ago, are the big fraud cases? It is not the ordinary person who has been scammed out of a few hundred or a few thousand. The concentration is always on the very big cases, which leaves an awful lot of people feeling neglected, because they feel that nothing will ever be done about their particular example of fraud.

Karl Laird: We may come on to this, but there is a broader issue there in terms of English law's ability to hold corporates to account effectively for wrongdoing. That may be an issue that we come on to.

The Chair: We will get to that in a moment.

Mark Fenhalls: You are right to use the word "neglect", and it is important when thinking about what fraud means to the public, the scale of it and where it is. In a sense, society as a whole has, over the past decade or more, tried to turn a lot of this into a cost of business. There is a real issue for us as a society as to who we make the gatekeepers in relation to all these issues. Are we making them the companies, banks,

building societies, tech companies? Where do we create liability for being the gatekeepers?

Running through this entire area, from the very small-scale simple frauds to the complex bigger frauds, it is extremely difficult for society to tackle the practicalities of this area and to outsource. How useful we think it is is an important question for us to be open about. We do not outsource where there has been a stabbing; we have the police to do that. This area, above all, creates some real challenges for us as to where we apply our resources, what we do and how we do it.

Lord Browne of Ladyton: I come back to the cost of business point, which is important because almost all businesses recycle that back to the customer. On the legal framework, is this the right place to ask about disclosure? We have written and other evidence that disclosure is so cumbersome that it causes investigations to grow exponentially and it takes up a lot of time. Do you have views about that, from your experience? You do. Good. Can you share them with us?

Mark Fenhalls: Of course. The Act was designed around a very specific problem that was pre-digital. It revolved around a warehouse of documents—notoriously, the Jubilee Line fraud—and the absolutely colossal volume of paper there, and the rules in place at the time that caused a vast diversion of resources. Therefore, the Government decided back in the mid-1990s to try to make the prosecution the gatekeepers of this material, so they created the structure of the Act.

It takes us back to the privacy issues and the control of information and of data. When I began and phones were first downloaded, the average phone download was 70 pages of just text messages and a list of calls. Now your average phone download is between 10,000 and 30,000 pages. That is because people live their lives on their phones. So there is plenty of grief around doing it, but there is no human way to search any of this stuff. The truth is that we have to work through an awful lot more thought about how issues are narrowed, how phones and computers are searched, in order to give people a chance to have a fair process.

It takes me back to the data question and the criminal justice exemption that I was talking about before. I defended a case last year where there were a lot of computers. The judge accepted in due course that it was impossible for the prosecution to do the filtering exercise, so we were given access to all of them. The defence lawyers used our data and our search tools. and we found what we wanted to find, but it was because the judge was persuaded in a particular case to depart from the norms that we were able to make sure that the trial took place.

I think there is a fear on the part of the state that if somehow the nasty, rotten defence community gets hold of this kind of information, there will be some dreadful thing and the world will fall apart. That is not the case. If we can get the disclosure process policed properly using that part of the Criminal Procedure and Investigations Act, some of this might go away. We should certainly try.

Lord Browne of Ladyton: There is a review of disclosure going on at the moment, which hopefully will report before we have to report back. There is an irony in this, because algorithms are part of the problem as far as fraud is concerned. If algorithms turned out to be part of the answer, that would be good.

Karl Laird: I will add that technology has a role to play here too. The example I would give you is the deferred prosecution agreement that was agreed between the Serious Fraud Office and Rolls-Royce. In that case, for understandable reasons, there was a huge volume of data and an AI program was used to go through it. That is obviously an extreme example, but I do wonder. Technology, as you say, is part of the problem, but it also can be part of the solution.

Mark Fenhalls: Can I give a practical example? If I may say so, it is quite important not to be distorted in our views by Karl's extremely accurate and perfectly good example. If you are thinking about a police officer dealing with somebody, a suspect in the cells, and wanting to narrow the issues and to know what he or she should not do with the phone that is in front of them, or the computer that they have seized in a search, you have to find a way to give them the tools to do the right thing and to get through that process so that it does not clog up the system.

I suspect that you would find universal support for the idea that if you have an experienced solicitor in a police station—which does not exist; hopefully some of the other changes going on will bring that about—that solicitor can gain the confidence of a client, can narrow the issues, can say to the police officer, "On the phone they communicate in the following way. Can you please download that particular kind of material from the phone? We don't need any of the films, we don't need any of the music, we don't need any of the photographs or whatever else".

If the tech is then available to the officers to have that informed conversation at that stage, early on, they can still safeguard the interests of the public, the complainants and the witnesses. What they find much more challenging is if they have to seize all this material, filter it using their own discretion and their own judgments, guessing what the defence wants or might need, that just builds in spectacular challenges.

Lord Sandhurst: I will ask you in a moment about the failure to prevent, but it occurred to me, listening to the evidence, that there are two ways of dealing with this. One, of course, is preventing fraud in the first place, or making it more difficult, which is what we have been talking about. The other is resources and training. Should we be recommending that money has to be spent on resourcing and training the police and the CPS to deal with this?

Mark Fenhalls: Yes, but we face a difficult time as a country, do we not? There will not be a period over the next few years when it is very attractive for any of those who are making decisions about resources to think that we must throw more money at this.

Lord Sandhurst: I would interrupt that to say that the billions of pounds that we now read are being taken by fraud would justify that, would it not?

Mark Fenhalls: It might well do. It would be very useful to have a true understanding, breaking down where all those costs lie. There might be a very big difference between, let us say, the interests of the banking industry and the telecoms industry. If there is a deficiency in the telecoms industry or a technology that they have involving the bombarding of text messages and whatever else it is that results in fraud to a bank account, who are you asking to police that? Who is the gatekeeper that Parliament wants to take action here? Do you wish it to be the technology company, the telephone company, the computer company, or does it fall upon the bank? Where should the real safeguards be? Yes, we need to think this through, and I am not quite sure that I have the experience to know where that answer should fall.

Q205 **Lord Sandhurst:** I will ask my next question of Karl, and you can pick up things that Mark has said. The Law Commission is reviewing corporate criminal liability. There are three limbs to this. First, what do you think about the instruction of a "failure to prevent" offence? That is being contemplated in the context of economic crime. "Failure to prevent" as a concept is now on the cards. How would you see it? Would it in fact incentivise platforms and telecoms companies in different ways to do something, where they have the ability to do it? Would it act as an incentive, and what might it look like?

The Chair: Those are all questions for Karl to consider this morning.

Lord Sandhurst: I tried to put it into three parts, and I think you have had notice of the line that we are going down.

Karl Laird: As a matter of principle I have no problem with "failure to prevent" offences. Of course, there has been a "failure to prevent" offence in English law now for over a decade, the offence in Section 7 of the Bribery Act. What I would say is that the term "failure to prevent" is a monolithic term that fails to appreciate that there are two different models of offence that we are talking about. There is the offence in Section 7 of the Bribery Act, which is concerned with failing to prevent bribery. In order for that offence to be committed, the employee or the person associated with the company must be acting with the intention of benefiting the company. That is an element of the offence. The second version of the offence is the one that is found in the Criminal Finances Act, which concerns the facilitation of tax evasion. That offence does not contain that same requirement.

What may seem like a technical difference is important in terms of the scope of the offences and the types of conduct that they will encompass. If we are going to go down the route of "failure to prevent" offences—failure to prevent economic crime, for example—first, we need to be clear about what model of the offence we are going to rely on, which is important for delineating its scope, but also what we mean by economic

crime. I am not sure that there is a precise definition of economic crime. Would we confine "failure to prevent" offences to fraud and money laundering? If so, why not failure to prevent other offences? There would have to be a principled reason for why we would circumscribe the applicability of the offences in that way.

In principle, I do not see a problem, but there are nuances that would need to be ironed out.

Lord Sandhurst: If we are looking at trying to prevent stuff coming down my telephone or people intercepting my emails, or that line of stuff, do you have a preference for the model of "failure to prevent" if you had to opt for one or the other?

Karl Laird: There are two possible answers there, one that is based on principle and one that perhaps is more pragmatic. The principled answer is: why should a corporate be liable for its employees committing criminal offences if they are on a frolic of their own? Why would we impose liability on the corporate in those circumstances? However, if that is the route down which we go, it will make the offences more difficult to prosecute, so there may be practical implications for that particular model of offence. We do not have a sense of how easy those offences would be to charge, because the "failure to prevent" offence in the Criminal Finances Act to my knowledge has never been charged. It has not been tested in the crucible of the Crown Court yet.

Lord Sandhurst: Is it in fact better to make this a regulatory burden, and go that way?

Karl Laird: On the point that was made earlier about the public's perception of fraud and their expectation, going down the regulatory route in one sense might be more straightforward, and it would enable us to circumvent the issues that we face in attributing criminal liability to corporates in English law. That would be the benefit, but from the public's perspective it would seem somewhat incongruous to have the employee being convicted of a criminal offence, and to have the corporate for which they work and which they may have been acting to benefit be committing a regulatory offence, which obviously would not attract the same stigma as a criminal offence, even though the penalty might not be dissimilar.

Lord Sandhurst: The penalty might be enormous.

Karl Laird: It might be enormous, but the penalties can be enormous for the "failure to prevent" offence in the Bribery Act, as we see in the deferred prosecution agreements.

Lord Sandhurst: If you do not bother with having it as a specific criminal offence to prevent fraud but you make it a strong regulatory framework and say, "Strict liability, but you can show that you took reasonable steps. But unless you do, fines and compensation will follow", might that not swing with the public?

Karl Laird: I would make two points. First, who will be responsible for enforcing this regulatory framework? If it is a crime, it is the responsibility of the police, it is the responsibility of the Serious Fraud Office. If it is a regulatory framework, who would we expect to investigate and ultimately prosecute these offences? I do not know the capacity of the FCA or its appetite to engage in this. That would be a matter for the FCA, obviously.

Second is a more general point about "failure to prevent" offences more broadly. That is not to lose sight of the impact that these offences have on corporates. When we think of these offences we tend to think of huge multinational corporations that can absorb the cost of putting compliance regimes in place. As has already been mentioned, they will most likely transfer the cost of compliance to their customers. That may be true of bribery, because bribery is an offence that tends to be limited to particular sectors and particular companies in particular sectors working in particular jurisdictions. If we were to have a broader failure to prevent fraud offence, the regulatory burden of that offence would potentially be felt most acutely by SMEs, much smaller companies, which may not necessarily have the means to put in place the sophisticated anti-fraud policies that we would necessarily expect.

Mark Fenhalls: I of course understand why "failure to prevent" appears a very attractive option. It takes us back to the gatekeeper conversation earlier, but I am sceptical as to the evidence of the effect of the two offences that we have had so far. I do not know if there is any less bribery going on because of the offence. I do not know if there is any less tax evasion going on because of the offence. Therefore, I would ask what the purpose is of this legislation. I know that collectively Parliament legislates because that is what it can do, but is it really going to make a difference? I would be concerned and anxious about it becoming an excuse for not enforcing, investigating and acting: "We have done that, so we can put this on the backburner for a little while". So where do you go? If you start saying that this is good, do we have failure to prevent pollution next? I do not know.

Lord Sandhurst: Water companies have to take steps.

The Chair: Baroness Bowles has done a lot of work in this area, too.

Q206 **Baroness Bowles of Berkhamsted:** Yes. We have got into quite an interesting discussion here, because, as Mark has said in referencing pollution, you get beyond what we are looking at at the moment, which is fraud, and into whether corporations in general should have a better duty of care or some other thing. If something bad happens, as it often does, and the company has been pretty negligent because it has happened, there rarely seems to be very serious comeback on them. The directors cannot be held to account because of mens rea and the difficulty in providing that unanimity of the directing mind and so forth. Is there not a hole where there could in fact be fraud or many other things and something one could do to close that hole?

Karl Laird: I agree that there is a problem in English criminal law as to how we hold corporates to account for criminal offences. As has already been pointed out, English criminal law still clings to this anthropomorphic conception of companies, and the only way we can attribute criminal liability to companies is through their directing mind and will.

That has two implications. The first is that it may encourage directors to distance themselves from wrongdoing so that the company cannot be held liable if it ever comes to light. The second is that that model makes it easier to prosecute small companies with relatively simple corporate structures, but it makes it much more difficult to prosecute corporates that have very complex corporate structures. So I agree that there is a problem in English criminal law that needs to be solved. Frankly, it is a problem that needs to be solved through legislation.

The courts have made very clear that the identification doctrine is going nowhere, so as a matter of common law the law has become crystallised and will change only through legislative intervention. I know that the Law Commission is examining that at the moment. The seeds of a more flexible approach are evident in Lord Hoffmann's judgment in the Privy Council in the Meridian case, a flexible approach that better recognises the complexity of corporate structures. I wonder whether consideration should be given to codifying Lord Hoffmann's much more flexible approach in legislation and sweeping away with the identification doctrine, because I do not think that it is fit for purpose.

Mark Fenhalls: Can I just say that I am not going to commit to a Bar Council view on corporate criminal liability today? The Law Reform Committee is working with the Law Commission. In due course, when our paper is complete, if I may I will send it through to the committee. We will try to capture there the range of different issues as far as this is concerned.

Baroness Bowles of Berkhamsted: There are other countries—obviously they are not necessarily running exactly the same law as us—where if the fact is that the company is benefiting from whatever has gone on, there is the possibility to prosecute them. The US has a slightly different strict liability regime, but they have mechanisms in Australia to try to get at some of these things, and I am quite a fan of them.

I was also wondering how much Section 4 of the Fraud Act could be used in relation to abuse of position. The all-powerful corporates have many ways in which they can trap customers into unfair things. We have had examples in banking where the drive for profit has meant that individuals in companies have engaged in some very bad practices, but the companies have largely distanced themselves from them, although it was their incentive policies and their drive for profit that have caused them. Can you use Section 4? You are getting on to anti-competitive behaviour as well here. How else could that section be used? Has it been used?

Mark Fenhalls: I do not know how widely it has been used. It would be a useful question to ask the Law Commission, because it will get a

properly reasoned, balanced, evidence-based answer. Certainly, we will look at it as part of the paper we provide it with, but I do not have a simple answer to your question.

Baroness Bowles of Berkhamsted: Do you see that there is injustice going on and that there is popular demand that something must be done?

Mark Fenhalls: I quite understand. In a sense, that is the thrust of all our evidence before you this morning and our concerns about what should be done. What underpins both my evidence and Karl's evidence, if I may say so, is that we want effective action, rather than simple political solutions. That is why we keep saying, as I said a few minutes ago, that we do not know how much "failure to prevent" has had an effect on levels of bribery or tax evasion. I do not know if anybody knows the answer to that. While we are looking at what corporate liability should be, some careful thought should be given as to how, on best evidence, there would be a change in behaviour. There is no point legislating just for the sake of it if we are not going to enforce a new set of rules.

Lord Browne of Ladyton: This is my personal view. I will share it with you, because I hope there is some merit in it. We are commissioned to look at the Fraud Act, job done, and digital fraud is very much a work in progress. Overwhelmingly, my sense of the evidence we have received is that there is a modern approach to this. If something serious goes wrong in any institution in this country, the first sentence in the press release and response to it is, "We take this issue very seriously". I think almost everybody who hears that thinks, "Well, you don't, because if you did, it would not have happened".

We have been treated to evidence from people who operate the important elements of that digital infrastructure, and every time they come in front of us their first sentence is, "Fraud is a priority for us". In one case we interrogated somebody about where it was reflected in the terms and conditions; the word "fraud" was never there in 80 pages of incomprehensible terms and conditions.

There is something to be said for trying to disturb that permissive culture. If I was a fraudster looking at this, I would say, "This is a permissive environment. I can go in there, because these people do not take responsibility for it". We frame this idea of having responsibilities as something that has a consequence for you, and that is your permission to allow this to happen with impunity. I do not think that is just a political response; it is a great statement from the country to say, "We're not going to put up with this any longer". If we do not have a way of doing it that way, do you have an alternative way that you can think of from your experience where we could achieve the same objective?

Baroness Kingsmill: May I make an intervention here, speaking on behalf of—

The Chair: Sorry, can we just let the witnesses answer, because we will come on to you in a minute.

Baroness Kingsmill: I have had my hand raised for some time, but people in the room get priority, I am afraid.

The Chair: No, sorry, we cannot see hands on that one. Let me allow Mark to answer and then we will come to your question.

Mark Fenhalls: Perhaps there is something to look at in terms of directors' responsibilities. I do not know the answer to your question. I agree that it is a critical problem, and I am simply not committing to a public position on what the answer is. If it was in the obligations of a director to deal with a certain package of things, and there was an enforcement mechanism to disqualify them as a director for the next X years, think how many people running big companies would have to find something else to do. I do not know if that would be worth considering.

Q207 **Baroness Kingsmill:** I want to make the point that the Bribery Act has worked quite considerably, I think. I sit on the board—until recently even more so—of some very large international companies such as telecoms, energy, retail, banking, and the Bribery Act has worked in the sense that it modifies the behaviour of organisations, which may be one reason why there have not been many more prosecutions. It modifies the behaviour because they have a reporting requirement, and they have a fear of the reputational risk of being engaged in that sort of thing. The behavioural changes that they undertake are extensive training and reporting on the level of training. Do you think that possibly the same sort of requirements in relation to fraud would work, especially since many corporations suffer losses as a result of fraud because they reimburse their customers in many respects?

One of the things that we have been looking at significantly is the legal response, which of course is the requirement of the terms of this inquiry, but if we want to modify the behaviour of corporates, there are ways other than the risk of prosecution. I would like your response to that before I tackle the question I have been allocated.

Karl Laird: Before dealing with that particular question, can I add something about the effectiveness of the "failure to prevent" offence in the Bribery Act? If there is a "failure to prevent" offence, there is the option of the SFO negotiating a deferred prosecution agreement with the corporate, and billions of pounds have entered the public coffers through disgorgement and fines because of deferred prosecution agreements in the context of failure to prevent bribery. Thinking about this in pounds and pence, that is something to not lose sight of—that if there is a failure to prevent fraud, that is the mechanism or the conduit through which the SFO can negotiate a DPA with a corporate, so it would broaden the SFO's capacity to enter into those kinds of agreement with the disgorgement and the fines that will follow.

In terms of changing corporate culture, yes, corporates must now have antibribery policies in place and potentially will be punished for failing to do so if it transpires that their employees are committing bribery. I alluded to this earlier: bribery is a very particular type of offence. It is

focused on certain sectors and companies that operate in certain jurisdictions. Fraud is a much broader type of offence, and it encompasses a much broader spectrum of wrongdoing.

It is one thing to say that huge multinational corporations can have in place very sophisticated antibribery policies and expect their employees to adhere to them, but I wonder how that would translate to small SMEs that find themselves having to have anti-fraud policies in place and how that would impact upon their profitability and potentially their viability.

Baroness Kingsmill: Would it not be helpful if such offences were directed particularly against corporates that profit from it? For example, telephone companies can profit from some of the fraudulent calls that are made to customers. When it comes to punishment, sometimes you must look for the people with the deepest pockets and direct some of these offences particularly to organisations that potentially profit, albeit unintentionally, from fraudulent activity.

Karl Laird: I wonder whether, if there was a failure to prevent fraud offence, there would be the desire to go after low-hanging fruit. Why prosecute a multibillion-pound corporation that can afford very expensive lawyers when the alternative is to prosecute a relatively small SME that does not have the deep pockets to afford that sophisticated legal advice? I wonder whether that would be an issue with a failure to prevent fraud offence—not targeting the telecommunication companies as you have described, but companies that are perceived as low-hanging fruit.

Q208 **Baroness Kingsmill:** We have heard evidence to suggest that jury trials are less effective because of the complexity of digital fraud cases. Do you think that specialist courts would be a good idea, rather as they are for competition cases, which are also extremely complex and are sometimes not dealt with or were not dealt with properly in the regular courts?

Mark Fenhalls: The short answer is no. Every jury I have ever dealt with in the last 20 years with a complex fraud has understood exactly what the issues are. It is critical, in my view, that they are permitted to continue to try these kinds of cases. There is no comprehension issue. There is a resource issue of space and time. This is the wider question for society. If you think in the context of the post-pandemic—hopefully post—backlog that we are dealing with in the courts when you are balancing different priorities, it is understandable at the moment if judges say, "The case with the child witnesses needs to be tried. The case with the murder needs to be tried".

There are fraud cases like that get pushed off into the distance, and I am afraid that backlogs contribute to the general problem and the public's sense of neglect. It takes us back to the question of why people do not report fraud. They do not report it, because they do not think anything significant is going to happen, and if they look at the delays built into the system and the structural problems around them, they have good reason for saying that. The chances of a fraud being reported, investigated and

prosecuted are pretty small on the numbers. The answer, in my judgment, is that it is not a problem of complexity.

We have in Southwark Crown Court a fantastic court, where there are a lot of specialist judges who deal with most of these big, complicated cases and the judiciary works hard to put experienced judges in place around the country to deal with the big, complicated cases. I do not see the same problem, and I have certainly seen no difficulty at all with jurors understanding all the material. We spend our lives making sure that it is in accessible language, and if they do not understand, they ask questions and they soon do.

Karl Laird: I agree, and add that the Court of Appeal deprecates any suggestion that jurors are incapable of understanding fraud cases. I can think of one Court of Appeal j*udgment where the Court of Appeal was very clear to be seen not to agree with the trial judge's suggestion that the jury in the fraud had reached the limits of what they were capable of understanding. The Court of Appeal made the point that Crown Court judges have case management powers in the Criminal Procedure Rules that enable them to manage these kinds of cases, and it will be incumbent upon the trial judge to ensure that the jury understands the prosecution.

Mark Fenhalls: There is lots of other complicated evidence that they understand too. They are perfectly capable of understanding DNA evidence or complicated other bits of science, and they do it very successfully.

Baroness Kingsmill: I agree with you, in the sense that it all depends on the evidence that is put before them and how it is explained. On the other hand, it has helped, in the competition area, to develop specialisations—advocates who understand the issues and know how to explain them very well, judges who understand them and have experience. There is an argument that it increases the profile of these cases and there is a pool of experts who are attracted to this area of law. That is an argument that specialist courts might work.

Q209 **Lord Sandhurst:** If we look at scams, not the Fraud Act, this is not the SMEs; this is access by the fraudster to the punter, and the fraudster must come through something like a search engine, telecoms, ISP and so on. There is a range of them. They are the big people. Forget about prosecuting them. You may want to prosecute them, but why not have a regulatory regime that says, "If this happens, you are liable unless you have taken steps to know your advertiser", for example?

Mark Fenhalls: On a very personal level—it is not a collective view—I have no difficulty with that. We all get the benefit of these spectacular services. We all pay for them, and in a sense we are collectively insuring ourselves. I would rather, if I may say so on a personal level—it is perhaps controversial—that there was less in the share price and in the rewards and more in the protection for the public who are using them. If I was a politician, that is what I would be trying to achieve.

Lord Sandhurst: Thank you. An academic view?

Karl Laird: I do not see any problem with that. Again, the point I would make is the practical one that I made earlier about enforcement. Whose responsibility would it be to enforce this kind of regulatory regime? Would it be Ofcom in the telecommunications sector? Would it be the regulatory bodies that are responsible for enforcing these regimes?

Lord Sandhurst: I am looking at it from a regulator's point of view, rather than the criminal courts.

Q210 **Lord Vaux of Harrowden:** We hear that most fraud is cross-border and a lot of it comes in from other countries, and that when investigated it comes to a grinding halt. How do we get to the overseas fraudsters, and how can we bring them to justice in any way to solve the problem?

Mark Fenhalls: The elephant in the room is that Brexit has made it harder. That is the reality, as far as Europe is concerned. We must work very hard to be a trusted international partner and build bilateral relationships everywhere we can. We must have the mechanisms in place so that local judicial systems and local police systems, wherever people are, are willing to co-operate.

The Chair: One of the suggestions in the memo that we saw this morning was about the Fraud Act and perhaps the extraterritoriality provisions being amended. Karl, you mentioned extraterritoriality in the context of the Computer Misuse Act.

Mark Fenhalls: Karl is much better for dealing with that. I will answer by saying that that gives you something in terms of effect, but it does not necessarily mean that you get hold of the person in whichever country it is that has been doing it, or indeed trace the money that has gone to a particular country in terms of getting redress. Given where we are now, we must create the international systems as best we can through bilateral agreements everywhere to try to get that co-operation and reciprocity.

Karl Laird: The territorial ambit of the offences in the Fraud Act is exceptionally broad. Strictly speaking, an individual in the United States who sends a fraudulent email to someone in England and Wales intending to cause them a loss commits an offence under the Fraud Act. It is difficult to see how the territorial ambit of the offences could be any broader. The problem, if there is one, is a practical one, as Mark says: how do we bring that person to justice, given that, prima facie, they are committing an offence contrary to English law?

Mark Fenhalls: I will give you one tiny practical illustration. Some of the computer companies—this came up in a murder case I prosecuted several years ago—will give the police live access to telephone data if they think that somebody may still be alive but is missing. As soon as there is evidence that somebody is dead, they close down and do not co-operate in the same way. It becomes an exercise in the labours of Sisyphus to try to get the data out of the foreign technology company that is the

custodian. Unpicking those kinds of blockages would be a very significant improvement to the police resources.

Q211 **The Chair:** You have given us some helpful evidence this morning. Is there one final particular key recommendation or item that we have not covered, or one thing that you want to bring to our attention that you think we should include in our final report? Mark, is there one particular key recommendation to government on this?

Mark Fenhalls: I would like the criminal justice exemption relating to data, however the best way to tease that out is. That seems to me, in my practical experience, to be infinitely the most important thing that would make the current systems work better.

Lord Browne of Ladyton: Like most of my questions, this is an observation. I am persuaded that your experience, both of you, justifies a conclusion that the system is capable of dealing with this and that it does not need to be fundamentally changed, but we should bear in mind that we have just gone through more than a decade's experience of courts being fooled by false evidence coming out of computers that was possibly just dishonestly presented to them, with the result that 750 or more sub-postmasters were convicted, lives were destroyed, people killed themselves, and now we are picking up this massive bill of compensation for them. It is not very convincing to say that the system can be capable. All these people were convicted in courts—to be fair, not all in the same level of court as you work in—and it was a judge who interrogated this properly and who discovered the misrepresentation of the evidence. The justice system produced the answer, at the end of the day, but we have this terrible history.

The Chair: That took a long time to get there. I will not ask you to comment on that, but, Karl, was there one final recommendation from your evidence?

Karl Laird: We have spoken a lot this morning about the enactment of new criminal offences. My one recommendation is to get rid of the common law offence of conspiracy to defraud, not to abolish it without replacements, but I do think it is extraordinary that we still have an offence in English law that criminalises conduct between two people that would not even be tortious if one of them were to engage in it. I am not saying that it should be abolished without replacement, but it is extraordinary that that offence still exists in English law.

The Chair: That opens up another level of questioning, and is particularly interesting in light of the memo that we received and particular recommendations made to the MoJ ahead of that memo. Perhaps we might follow that up privately with you, given that what you have just said is quite different from the conclusions that the MoJ has drawn in that memorandum. I can see that Mr Fenhalls wants to come in very briefly on this.

Mark Fenhalls: Conspiracy to defraud is a supremely practical, useful, effective tool.

The Chair: Yes, which is the point made in the memo.

Mark Fenhalls: I would be extremely reluctant to open this debate without having a very clear set of proposals as to what the supposed alternative would be.

The Chair: Thank you. That sounds like something further to follow up with you both, but thank you very much in the meantime for the very helpful evidence and for the open way in which you have shared your thoughts this morning.