



House of Commons
Home Affairs Committee

Terrorism Detention Powers

Fourth Report of Session 2005–06

Volume II

Oral and written evidence

*Ordered by The House of Commons
to be printed 20 June 2006*

HC 910-II
Published on 3 July 2006
by authority of the House of Commons
London: The Stationery Office Limited
£16.50

Home Affairs Committee

The Home Affairs Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Home Office and its associated public bodies; and the administration and expenditure of the Attorney General's Office, the Treasury Solicitor's Department, the Crown Prosecution Service and the Serious Fraud Office (but excluding individual cases and appointments and advice given within government by Law Officers).

Current membership

Mr John Denham MP (*Labour, Southampton, Itchen*) (Chairman)
Mr Richard Benyon MP (*Conservative, Newbury*)
Mr Jeremy Browne MP, (*Liberal Democrat, Taunton*)
Mr James Clappison MP (*Conservative, Hertsmere*)
Mrs Ann Cryer MP (*Labour, Keighley*)
Mrs Janet Dean MP (*Labour, Burton*)
Mr Shahid Malik MP (*Labour, Dewsbury*)
Margaret Moran MP (*Labour, Luton South*)
Gwyn Prosser MP (*Labour, Dover*)
Bob Russell MP (*Liberal Democrat, Colchester*)
Martin Salter MP (*Labour, Reading West*)
Mr Richard Spring MP (*Conservative, West Suffolk*)
Mr Gary Streeter MP (*Conservative, South West Devon*)
Mr David Winnick MP (*Labour, Walsall North*)

The following Members were also Members of the Committee during the inquiry:

Colin Burgon (*Labour, Elmet*)
Nick Harvey (*Liberal Democrat, North Devon*)
Nick Herbert (*Conservative, Arundel and South Downs*)
Steve McCabe (*Labour, Birmingham Hall Green*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the Internet via www.parliament.uk.

Publications

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the Internet at www.parliament.uk/homeaffairscom.

Committee staff

The current staff of the Committee are Dr Robin James (Clerk), Mr Mark Etherton (Second Clerk), Kate Akester (Adviser (Sentencing Guidelines)), Martha Goyder (Committee Specialist), Ms Arabella Thorp (Inquiry Manager), Mr Ian Thomson (Committee Assistant), Jenny Pickard (Secretary) and Alison Forrester (Senior Office Clerk).

Contacts

All correspondence should be addressed to the Clerk of the Home Affairs Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 3276; the Committee's email address is homeaffcom@parliament.uk.

Witnesses

Tuesday 7 February 2006

Page

Dr Eric Metcalfe, Human Rights Policy Director, JUSTICE, **Ms Shami Chakrabarti**, Director, Liberty, **Ms Gareth Peirce**, Birnberg Peirce Solicitors and **Mr Tim Owen QC**, Matrix Chambers

Ev 1

Tuesday 14 February 2006

Lord Carlile of Berriew QC

Ev 16

Professor Ross Anderson, Foundation for Information Policy Research, **Mr David Lattimore**, Technical Manager, Digital Crime Unit, LGC Ltd and **Mr Peter Sommer**, London School of Economics

Ev 25

Mr Daren Greener, Systems Technology Consultants Ltd, **Mr Vinesh Parmar**, Telecoms Forensic Technical Manager, Digital Crime Unit, LGC Ltd and **Mr Gregory Smith**, Principal, Trew & Co

Ev 30

Tuesday 28 February 2006

Andy Hayman QPM, Assistant Commissioner and **Peter Clarke CVO OBE QPM**, Deputy Assistant Commissioner, Head of the Anti-Terrorist Branch and National Co-ordinator of Terrorist Investigations, Metropolitan Police Service

Ev 35

Tuesday 21 March 2006

Rt Hon Charles Clarke MP, Secretary of State for the Home Department

Ev 56

List of written evidence

	<i>Page</i>
1 Association of Chief Police Officers of England, Wales and Northern Ireland (Terrorism and Allied Matters) Committee and the Metropolitan Police Service	Ev 70
2 British Irish Rights Watch	Ev 73
3 Campaign Against Criminalising Communities	Ev 76
4 Robert Czapiewski	Ev 78
5 Foundation for Information Policy Research	Ev 79
6 JUSTICE	Ev 82
7 David Lattimore	Ev 87
8 Liberty	Ev 91
9 Mark Morris	Ev 94
10 National Technical Assistance Centre	Ev 96
11 Mr Vinesh Parmar	Ev 97
12 Evan Price	Ev 98
13 Secretary of State for the Home Department	Ev 100 : Ev 102
14 Gregory Smith	Ev 102 : Ev 109
15 Peter Sommer	Ev 110 : Ev 114
16 Chris Sundt	Ev 115
17 UKERNA	Ev 118
18 Professor Brian Collins	Ev 119
19 Daren Greener	Ev 121
20 Metropolitan Police Service	Ev 125

Oral evidence

Taken before the Home Affairs Committee

on Tuesday 7 February 2006

Members present:

Mr John Denham, in the Chair

Mr Richard Benyon
Mrs Ann Cryer
Mrs Janet Dean
Mr Shahid Malik

Gwyn Prosser
Mr Richard Spring
Mr David Winnick

Witnesses: **Dr Eric Metcalfe**, Human Rights Policy Director, JUSTICE, **Ms Shami Chakrabarti**, Director, Liberty, **Ms Gareth Peirce**, Birnberg Peirce, Solicitors, and **Mr Tim Owen QC**, Matrix Chambers, gave evidence.

Q1 Chairman: Can I welcome you to this first session of our Inquiry into Terrorism Detention Powers. Just by way of background, obviously the House of Commons voted before Christmas on proposals to extend the period of detention without charge to a maximum of 90 days and voted to reduce that period to 28 days. There was considerable discussion at that time about how well or how poorly the case for an extension for detention powers had been made and, notwithstanding the fact that the House of Commons had already voted, this Committee decided to hold a short inquiry into the case for detention powers and the alternatives that have been put forward, and so on. We hope certainly that this inquiry is not simply of historical interest because, as we know, there will be a proposal, in a year or so's time, to produce perhaps a consolidated Terrorism Act, pulling together all the various different strands, and it seems very likely that, in some form or other, these debates around detention and the conduct of terrorism investigations will come back onto the political agenda. We hope our inquiry, inevitably it starts from a discussion which the House of Commons was having a few months ago, will be useful when we come to look at these issues in the future. Can I start by asking each of the witnesses if you could introduce yourselves, very briefly, for the record, then we will get under way?

Mr Owen: Tim Owen, Queen's Counsel, from Matrix Chambers, barrister, with experience of criminal and human rights issues.

Ms Chakrabarti: Shami Chakrabarti, Director of Liberty, the National Council for Civil Liberties.

Dr Metcalfe: Eric Metcalfe, Director of Human Rights Policy at JUSTICE.

Ms Peirce: I am Gareth Peirce, a solicitor who has spent a lot of her life in Paddington Green Police Station.

Mr Winnick: You have been impersonated in films as well.

Q2 Chairman: Thank you. I have a couple of opening questions which I am going to address to all the witnesses, but, in view of the time, if you agree completely with what the last person has just said

please do not feel the need to say it again. I will start off, if I may, with Shami Chakrabarti. Do you accept the basic contention that terrorism cases do present special features for the legal system and the criminal justice system and so, in principle, should be treated differently from other criminal cases?

Ms Chakrabarti: I think the first proposition that I would make is that terrorism is crime, and that is very important. If you remember, Mr Denham, the diatribe recorded by Mohammed Sidique Khan, who was one of the London bombers, one of the many things that he said was "This is a war and I am a soldier." I think one should always be careful, whether with political rhetoric or with political and legislative policy, not to allow a murderer to call himself a soldier. There are also dangers with any culture of exceptionalism, because I believe the threat is real and I think it may be long term and so there are grave dangers with a state of exception that could go on for a generation or several generations. That said, I do accept that some terrorist offences are likely to have very serious consequences. I think what is important is to be specific about particular operational problems and particular offences, rather than for people on either my side of the argument or the security side of the argument to talk about whether terrorism is so unprecedented that we have to change the rules of the game.

Q3 Chairman: In principle, this is acceptable, to have legislation which may be described as a Terrorism Act, but, nonetheless, we need to look very carefully at what it contains?

Ms Chakrabarti: When we do, I think one should make an important distinction between the substantive and the procedural criminal law. For example, in this country now we are well used to having specific offences that are terrorist offences; some people have concerns even about those. They tend to be broader in their ambit and at times they include reverse burdens of proof, and so on. Of course one has concerns about that, but the graver difficulty, in my view, is with undermining procedural criminal protections, in particular the presumption of innocence.

Q4 Chairman: Do any of the other witnesses wish to add anything significantly different from that?

Mr Owen: Speaking from the point of view of a practitioner, I think the answer to your question is, no, I do not see, from the way in which the criminal justice system has to operate, that it requires fundamentally different rules. Terrorist offences, firstly, range enormously in seriousness from, at the lower end, membership of a proscribed organisation right up to conspiracy to murder, and so on. In terms of the way the criminal justice system operates, the rules of evidence, the presentation of evidence, I do not see that there is justification for a fundamentally different approach. Investigation is perhaps a different matter.

Ms Peirce: I simply note the comment on the police officer's briefing, Andy Hayman, to suggest that Irish terrorists, rightly or wrongly called, presented a different problem. Certainly that was not the way it was ever put, in any prosecution of any Irish defendant, and at that point of time seven days was considered an extravagantly long time that was a great deal for any suspect to have to endure. I think I cannot accept the proposition that the threat has changed in degree or severity or quality or the factual basis, it is very, very similar, and the investigative mechanisms and powers, in my view, present almost identical problems for all concerned.

Q5 Chairman: I will come back to that in a moment, if I may, but let Mr Metcalfe have a say?

Dr Metcalfe: Operationally, I can see that it makes a great deal of difference to the way in which the police have to tackle suspected offences, but, legally speaking, I agree completely with what other panel members have said, legally it does not make any difference. Bearing in mind that the problem with talking about these things, in most of these terrorism cases, is the broad definition that we have under Section 1 of the Terrorism Act 2000. Under the terms of the Terrorism Act a terrorism case may involve a crop protestor committing criminal damage. It is perfectly correct for the police to address offences which involve the threat of large-scale loss of life, but it would be wrong to say that every terrorism case, as defined under the Act, necessarily would involve such a threat.

Q6 Chairman: Accepting the point which Dr Metcalfe has made, that the definition of terrorism is very broad, and actually Lord Carlile has been invited to advise the Government on the definition of terrorism, so if we can put to one side some of the more minor offences which can get caught up in the terrorism definition at the moment, Gareth Peirce, you said that you did not think the threat had changed in a significant way. We appear to be facing terrorists now whose central aim of terrorist action appears to be to kill as many people as possible as indiscriminately as possible. Is not that actually quite a significant change in the threat that we expect the police and the security services to protect us from, and that may require, in some way, those organisations to act differently?

Ms Peirce: I think, the IRA bombing campaign, which was directed, for the large part, against London over 25 to 30 years, it is quite wrong, retrospectively, to classify it as it was seen throughout by the police and the security services as anything other than exposing the citizens of London and the rest of the country to extreme danger. That was the way it was perceived. Whether or not it was conceded on occasion that the IRA sought to give warnings, I have to say, as a person who defended IRA suspects over many years, it was never put that way on prosecutions, it was always put that there was a high risk, or worse, of civilian casualties, all the time.

Q7 Chairman: That is perfectly obvious, that the IRA campaign did cause civilian deaths and, constantly, warnings or no warnings, ran the risk of civilian deaths. Nonetheless, is there not a substantive difference between that and the type of terrorist tactic which appears, as with the July bombings, to put the primacy simply on killing as many people as indiscriminately as possible? In practical terms, we look to the police and security services to protect us. Is it not the case that, faced with that type of threat, the measures they may need to contemplate will need to go further than were necessary in dealing with the IRA campaign?

Ms Peirce: I will split your question into two. I think one has to analyse, at some stage in our discussion, as to the appropriateness of the data we are considering, in relation to July 7, that is an important factor, what the police had to investigate, whether they used it properly or not. In terms of simply quantifying it, whether there is one death or 3,000 deaths, a bomb going off in a city, in my view, has to be approached with the same degree of seriousness of inquiry. I cannot see that the end result itself dictates a different form of investigation; all must be of the highest quality and the highest calibre.

Q8 Chairman: We will come on to the detail of this in a moment, but if part of the police argument is that some preventive measures are necessary, and obviously they are talking about detention powers, and we will go into that in detail, is it not the case that if what you fear is the attempt to kill of hundreds of people you may be justified in using a level of preventive measures that you would not have judged necessary when the danger was that somebody would be killed if a bomb warning was not acted upon? Would you really regard the two as exactly the same and there is no difference between the attempt to kill hundreds of people and the attempt to kill one person?

Ms Peirce: I regard the phenomenon we have faced in this country for at least 25 years, a phenomenon of bombings, carried out for political motives, to have been the most exceptional danger that any country could have been exposed to on a sustained level. I simply stick to what I say. Having experienced that and learned what we had to learn from that, I find it unjustifiable to do a quantum leap from an extended period of seven days to the level it is now.

7 February 2006 Dr Eric Metcalfe, Ms Shami Chakrabarti, Ms Gareth Peirce and Mr Tim Owen QC

Ms Chakrabarti: Forgive me, Mr Denham, I think there are aspects of this kind of discussion which are unhelpful, because it is too easy to make sweeping statements about “this is an unprecedented threat,” “the IRA were gentlemen bombers;” I exaggerate.

Q9 Chairman: It is not what I think anybody in the Committee has suggested to you.

Ms Chakrabarti: No, not in the Committee, but out in public discourse it is very easy to get into a situation which is very unpleasant for IRA victims, for example, and the idea of the Raffles gentleman bomber always leaving a calling-card, of course that was not true. Equally, this threat is complex too. I am prepared to accept that the threat has aspects of difference about it. I am prepared to accept that it is not people like me who have access to secret intelligence, that is the nature of secret intelligence. What I always say is that the rule of law is robust enough to deal with this threat or that threat and that the post-war human rights consensus, that is the rule of law that we are talking about here, the Convention Articles, the right to a fair trial, qualified interferences with privacy, even the provisional Article 15 of the Convention on Human Rights which allows for a temporary state of exception, these provisions were drafted by democrats after the second world war, Eleanor Roosevelt, Winston Churchill, and so on. These people were not naïve 1960s liberals, they had lived through the Holocaust and the Blitz and they came up with a framework that is still important today. It is against that framework that we and others should be examining this threat, or any new threat. There will be aspects of difference, there will be aspects of similarity; it is important to be specific about what is different.

Q10 Chairman: If we can be specific, what level of risk do you think we should be prepared to accept? This debate is, essentially, as you say, which of our established freedoms are we prepared to erode, by how much, in the face of the threat that we have got now? I think you are saying that the nature of the bomb threat we have now makes no difference, compared with the IRA fear, to that balance between freedoms. I suppose the question I am trying to pin you down to be specific about is what level of risk do you think we should be prepared to take rather than erode any of our freedoms?

Ms Chakrabarti: I would say that the framework for analysing this is all in the Convention. For example, one of the reasons why in public discourse people say frequently that these bombers are different from any other bombers is the concept of ‘suicide bomber’, which presents particular operational challenges and which is particularly uncomfortable for us because we find suicide difficult as well as the idea of murder difficult, so it is particularly unsavoury in our consciousness. Operationally, I have to accept, as a human rights proponent, that Article 2 of the Convention on Human Rights is an incredibly important Article of protection, but it is not absolute. For example, it allows for even the use of lethal force when strictly necessary to prevent an

atrocious. I accept that, in the specific context, that operational context, if someone were about to detonate a suicide device but not acting by remote control, you might have to use more force than otherwise you would do. One has to approach this issue with that level of specificity, rather than sweeping political statements of that, because we have suicide bombers now, it is too much risk, and therefore we sweep away fair trial protections, protections against arbitrary detention, and so on.

Q11 Chairman: Let us not go too sweeping in answer to these questions. Essentially, you say we should work from the Convention backwards; some other people in the debate certainly will say “Let’s work from the risk upwards and have a response that’s proportionate.” Mr Owen, or Metcalfe, do you have anything to add on this point?

Mr Owen: I think the relatives of those who died in Enniskillen, Omagh, Guildford, Woolwich, Birmingham or Canary Wharf would take the view that the IRA did not give targeted or clear warnings and I agree with what Gareth Peirce had to say about that. I just have a difficulty with Mr Hayman’s paper on this point. While, of course, on one view, the more people who are killed the more evil and wicked is the deed, but in terms of the threat, if you have a lorry loaded with three tonnes of home-made fertiliser being driven around London and left in a public place, with no or an inadequate warning, is it really suggested that the police would not, do their utmost to arrest at the earliest point to avoid the threat? I do not see, conceptually, how it really matters whether it is a suicide bomber or a lorry being driven, loaded with explosives. This is important because that sets the scene for Mr Hayman’s subsequent approach, because then what he says is, because you have to intervene at this prophylactic stage, at a stage where, in effect, he is saying, often you have no evidence at all, I just question that.

Chairman: I think witnesses have been very clear and consistent about the similarities they see between the current threat and the previous IRA threats. I do not think we need to go into that any further.

Q12 Mr Winnick: You mentioned, just for a moment, a number of atrocities carried out by the IRA. As far as Birmingham, which is near my constituency, is concerned, is it not the case that 21 were murdered in that terrible November in 1974, half of whom, I should say, Mr Chairman, were under the age of 25? Coming on to the justification that the police make for 90 days, you will have read the theoretical case study where the police use every kind of argument to say why, in all the circumstances, technical reasons given, and the rest of it, it is absolutely essential for the security of our country that the law provides for up to 90 days’ detention; you are not impressed, presumably, the four of you? Ms Peirce, were you at all impressed, although I suppose the answer is pretty obvious?

Ms Peirce: Fairly obvious, but I think it is absolutely tragic that Parliament took its decisions on the length of time without first having a pause for

investigation to get proper data, proper empirical data, as to what actually happens in police stations, the kinds of time and motion studies of how much time is used. In particular, in relation to July 7, I find it quite extraordinary that this whole debate and legislation, and once there is legislation in place there is never the same momentum to de-legislate, and, I fear, here we are, with 28 days now.

Q13 Mr Winnick: That was not quite my question, with respect, Ms Peirce, because we know your strong views and we have read your article, which has been circulated. My question really was do you see any merit—perhaps I could have put it better, and it would be my fault—whatsoever in the theoretical case study the police have given as justification for up to 90 days’ detention, any merit at all?

Ms Peirce: No, I see none, and I would argue for a retreat to seven days. I am sorry I digress but just to make one point very quickly. In relation to July 7, I believe that Parliament ought to have been provided, and still ought to be provided, whether it be privately or publicly, with what was known to the police beforehand about those who carried out the bombings, what police powers were used—

Chairman: I am sorry, I must stop you. I think it is very important, because we have a number of questions to cover, that you reply directly to Mr Winnick’s question about the case study.

Q14 Mr Winnick: I think we can work on the assumption that you see no merit at all in it. We can cut this pretty short, because obviously you are putting the opposition case, we will have the police in due course, therefore my questions are theoretical as well as discussing a theoretical case study. Do any of the four witnesses see any merit whatsoever, obviously what you have studied, in the case which the police have put forward? Mr Owen? Really, yes or no, you might say.

Mr Owen: I accept that the factual information, if you like, may well reflect the reality of what the police are up against, but I do not accept that the legal system, at the moment, is not capable of delivering a solution without going to 28 days, or even 14 days. I have got six points to make about it, but I know you do not want six points.

Mr Winnick: Not on this question.

Q15 Chairman: It would be useful to have the key points about the case study, and we could take that now?

Mr Owen: To give you the six points. The first has been dealt with. I think Mr Hayman’s paper greatly exaggerates the different nature of the threat. Secondly, it proceeds on the assumption that at the point of arrest the police have literally no evidence and the 14 days provides the first opportunity to commence investigation. Yet Mr Hayman’s case study assumes two months of surveillance, including probes, and one really questions whether literally nothing emerges from that. Thirdly, there is no factoring in of the, frankly, absurd consequences flowing from our statutory bar on the admissibility of intercept evidence. At the moment, of course, if you

know that intercept evidence is not admissible as evidence, you do not use intercepts in the way that you would if they were, and you use them for a purely intelligence background as opposed to an evidence-based background, and so really he does not factor that in. Fourthly, he suggests that at the point of charge the CPS must be in a position, in effect, to serve all its evidence and that the police are not permitted, at the moment, effectively, to continue to investigate; that is simply not the case. The current position, with any complicated terrorist case, is that the police and CPS in effect get at least six months to serve the papers. It means that a defendant has to wait six months before he can even make a dismissal application on the grounds that there is no evidence; so that is not reflected in Mr Hayman’s paper. Fifthly, it fails to acknowledge that at the post-charge stage, in other words, detention pending trial, the Crown Prosecution Service and the police get what I would say is a pretty easy ride from the courts. Bail is hardly ever granted in terrorist cases. Evidence can be, and is, served continuously throughout the remand process, in stages, sometimes right up to the day before the trial. As for custody time limits, which is the way in which post-charge detention is regulated, again there is an extremely generous approach by the courts. As long as the prosecution show that they are investigating continuously, in a diligent way, the judge will extend custody time limits, sometimes up to two years. I was involved in a case last year, for example, in which the trial is not going to take place now until April of this year. The arrests were in August 2004, almost two years earlier, with custody time limits consistently extended throughout. Lastly, I think Mr Hayman greatly exaggerates the benefits of interviewing as an exercise in evidence-gathering in itself, and he does not take account of the current Code of Practice, paragraph 16.5 of Code C, which enables interview post-charge in exceptional circumstances. Those are the six points.

Chairman: We will come back certainly to that post-charge interview question a little later on.

Q16 Mr Winnick: Thank you very much; that is very useful.

Ms Peirce: May I add one point to Mr Owen’s six points, in terms of what the prosecution has at its disposal, because the inference is, if you do not get someone while they are in the police station to admit or keep silent what they are being asked about, that the chance has gone. There is an entirely new procedure, which is much more stringent than it used to be, of a requirement on a defendant to give a defence case statement, in writing, before his trial, to the prosecution, which deals with every issue and every accusation in the case, and if he does not do that, or she does not do that, then it is a matter for comment and inference that the jury can draw, and that is missing completely from Mr Hayman’s analysis.

Q17 Mr Winnick: Dr Metcalfe, do I take it that, as far as the theoretical case study is concerned, you do not accept the police evidence?

7 February 2006 Dr Eric Metcalfe, Ms Shami Chakrabarti, Ms Gareth Peirce and Mr Tim Owen QC

Dr Metcalfe: Yes, that is correct, entirely for the reasons which Mr Owen and Mrs Peirce have given.

Ms Chakrabarti: Just briefly, Mr Winnick, because I do not want to accuse the police of bad faith on this, they write a hypothetical case study, based on their experience, they raise many of the real operational concerns that they have here and there, but they start from the premise that they suspect an event in 90 days; that is the operating premise of this exercise, and I could write the exercise and make it 100 days, or 200 days, or 10 years. A police officer could always do with more time, and of course we are talking about terrorism and you would like to have that time with the person detained. If you put it that way, it is an unassailable argument for completely dismantling fair trial protections.

Q18 Mr Winnick: Can I come to the crux of the matter, to a large extent at least, in this section of questions, the question basically whether the police should have any powers of detention without charges being made? Ms Peirce, as far as I recall, a few moments ago, said maximum seven days, am I not right?

Ms Peirce: That is a punishing amount of time for a suspect to be questioned, seven days.

Q19 Mr Winnick: As far as you are concerned, it should be simply seven days. Dr Metcalfe, in the evidence that JUSTICE has provided us with, on page two of your brief, you say, in effect, that 14 days is the maximum period you would be happy with. You differ, do you not, from what Ms Peirce has just told us; you are happy with 14 days?

Dr Metcalfe: No, we are not happy with 14 days.

Q20 Mr Winnick: But you are willing to live with 14 days?

Dr Metcalfe: In terms, we expressed a view that we thought 14 days was the maximum likely to be found compatible with the European Convention on Human Rights. That does not mean that we are happy with it.

Q21 Mr Winnick: What would you be happy with?

Dr Metcalfe: We believe that seven days, the original limit set down in the 2000 Act was the correct one and we did not agree with the extension, made under the 2003 legislation, to 14 days.

Q22 Mr Winnick: Regardless of the atrocities which occurred on 7 July and what may or may not have happened a fortnight later, the organisation which you represent has not changed its views at all?

Dr Metcalfe: We have made it perfectly clear that we recognise the operational difficulties but we do not see that makes a difference to the legal framework which was established.

Q23 Mr Winnick: So it is seven days; if you had your way, JUSTICE, it would be seven days?

Dr Metcalfe: It would be seven days, yes.

Q24 Mr Winnick: You indicated, nevertheless, as I have said, that you could live with 14 days, from your brief?

Dr Metcalfe: Yes.

Q25 Mr Winnick: Liberty's view?

Ms Chakrabarti: If you will forgive me, Mr Winnick, we are reluctant to enter into this approach.

Q26 Mr Winnick: I will try to put it differently. What we would like to know, as a Committee, is whether Liberty would be in favour of any form of detention without charges, apart from the original, what was it, two days?

Ms Chakrabarti: The requirement in law and in good constitutional policy is for someone to be charged promptly. Any extension of the pre-charge, and charge is a very important moment, and elsewhere you may ask us about lengthy periods of pre-trial detention in other countries, let us be clear about this, the right to know the charge against you promptly is a bare minimum, and a crucial bare minimum. If I am detained for a long time pending a complex trial where I am preparing my defence, the greater injustice is with being detained for a long time without even charge. From a counter-productivity point of view, this is essential, because the person who is detained, for many months or even, on occasion, into years, and then tried for a terrorist offence and acquitted is quite possibly celebrating at the court door, with a fantastic solicitor, like Mrs Peirce, standing by her side. The person who was detained for 90 days, or longer, pre-charge, and then sent home from the police station is not in such a celebratory mood, and the dangers to social policy and to operational policing and security work, I think, are desperately dangerous. I suggest that it is the job of parliamentarians to look at these issues and to look at the proportionality of the policy and to say that, before any extension in pre-charge detention is even entertained, all more proportionate, alternative policies should be explored. That, of course, is what you do not find in Mr Hayman's dossier, because that is not his job. For my sins, I used to be a Home Office civil servant; you would never have given advice in this unbalanced way.

Chairman: I must ask you to restrain your desire to give us the whole answer on every question, otherwise we will never make progress.

Q27 Mr Winnick: Mr Owen, do you take such a fundamental viewpoint as that which the others do?

Mr Owen: Can I answer your question in these two ways. Firstly, I agree with Gareth Peirce that I find it difficult to see how the average English judge would regard it as fair to admit evidence obtained by interview after a person had been held for more than seven days in custody, or certainly longer than 14 days, without any charge. Secondly, the most important legal restraint at the moment obviously is what the European Court of Human Rights has sanctioned. The position as set out quite recently in

the case of *Tannikulu v. Turkey* is that 10 days pre-charge detention was struck down as incompatible with the right to liberty in Article 5. And in *Brogan v. UK* four days six hours was struck down as incompatible, therefore needing a derogation from Article 5. I think there are difficulties, real difficulties, and I am by no means sure about 14 days ultimately being held to be compatible with Article 5.

Q28 Mr Winnick: I was going to ask about the Convention on Human Rights, but, as far as you are concerned, Mr Owen, do we take it that your views are just the same as those of your three colleagues?

Mr Owen: Yes.

Q29 Mr Winnick: Seven days?

Mr Owen: I think more than seven days without charge is unacceptable, yes.

Q30 Mr Winnick: Mr Owen, you say that you have considerable doubts about whether more than 14 days would not be a breach of the Convention on Human Rights?

Mr Owen: Yes. Of course, an important question—this leads on to another point about the involvement of the judges in the supervision—

Q31 Mr Winnick: Indeed, you would hope that would be the position, would you not?

Mr Owen: It is not a question of whether I would hope it would be the position.

Q32 Mr Winnick: Taking the view that you do, presumably, like the other witnesses, you would be happy, if Parliament agreed to a period longer than 14 days, surely, given that viewpoint, you would wish that to be a breach of the European Convention on Human Rights, it would make sense, would it not?

Mr Owen: Yes. I think it would represent an abandonment of a core principle.

Q33 Mr Winnick: That answers my question. Presumably, to cut matters short, because there are many other questions to come from colleagues, the three of you would be happy that, if Parliament did agree, at the end of the day, to a period longer than 14 days, it would be a breach of the Convention on Human Rights?

Ms Peirce: Yes.

Dr Metcalfe: Yes.

Ms Chakrabarti: Yes, Mr Winnick.

Mr Owen: Yes.

Chairman: I am sorry, but we need to move on now to some of the more detailed aspects of the issue: Shahid Malik.

Q34 Mr Malik: This is a question to all the witnesses. You will be familiar with Lord Carlile, and I am going to quote him; he says that he is “satisfied beyond doubt that there have been situations in which significant conspiracies to commit terrorist

acts have gone unprosecuted as a result of time limitations placed on the control authorities following arrest.” Do you think he is wrong?

Ms Peirce: I am completely unaware of a single example. If he gave his examples, it would help.

Dr Metcalfe: Can I say that I am very disturbed by the statements that Lord Carlile made in his report. As the independent reviewer of the terrorism legislation he is given access to closed information that is not made public. I am not in any way comforted by the fact that he has special access to information that other people do not have and then feels secure in making these statements about how happy he is about increasing the extent of terrorism legislation. I think it is profoundly dangerous, in a democratic society, for measures which infringe on fundamental rights to be justified in this way. President Truman once said that secrecy and democratic government do not mix and I hope that the Committee will bear that in mind when they have regard to these kinds of statements. I have great respect for the role that Lord Carlile is appointed to carry out and I think that he does it with great diligence, but I am deeply concerned that we should be justifying public policy on such a basis.

Q35 Chairman: Is your point that he should not make such statements, even if he is convinced that they are true, or that we should dismiss them because we do not know the basis on which he has made them?

Dr Metcalfe: We are in no position to second-guess someone when we do not have access to the evidence ourselves and, much as I trust Lord Carlile to carry out his role as the independent reviewer of terrorism legislation, I do not trust him to govern for us, and essentially this is what you are asking someone to do when you make statements of that nature.

Q36 Mr Malik: Basically, you and Gareth are making the same point, that because you do not know the examples, because of the privy nature of it, you think, on those grounds, it is not warranted?

Dr Metcalfe: Yes. I cannot place any weight on that statement, unfortunately, much as I might like to.

Ms Chakrabarti: It may be that silence would be even better than succinctness, and Mr Denham will forgive me for my lengthy remarks on other questions.

Mr Owen: I think you are going to have to deal with Lord Carlile in private and find out from him exactly what that is based on, and perhaps you will need a special advocate to cross-examine him in front of you who is party to the same material. The difficulty I have with this is that he is postulating a scenario in which there are lawful grounds to arrest this person, or persons, for serious offences, but 14 days have gone by and there is no evidence available which passes the Threshold CPS Test for charging in relation to any offence at all. Really I question whether that is true, and when you question Lord Carlile, I am not suggesting he is lying or acting in bad faith but it is a question really of testing the implication of what he is saying.

7 February 2006 Dr Eric Metcalfe, Ms Shami Chakrabarti, Ms Gareth Peirce and Mr Tim Owen QC

Mr Winnick: We will do our best.

Q37 Mr Malik: Your position basically is that you cannot see on what grounds this could be a legitimate comment to make?

Mr Owen: I just do not know. It is not fair perhaps, because I have not seen what he has seen, but I am saying that that is the implication of what he is saying and it seems a fairly extraordinary state of affairs.

Mr Malik: That is fair comment.

Q38 Chairman: This is useful, because this is the first session, because it does help us set up questions for later evidence sessions.

Ms Chakrabarti: Mr Owen tempts me back in, just briefly, because he reminds me of a really important point. Let us look at anti-terror legislation in the round, look at the full armoury at the disposal of the police and security services and look also at minor offences, precursor offences, acts preparatory, being a member of a prescribed organisation, etc., bicycle-taking, whatever it happens to be, there is a lot of criminal law on the statute book and you can take preventative measures, in a sense, by using lower-level offences.

Mr Owen: You might want to ask him whether there was intercept evidence available which they could not use, and that then leads to the question, was that sensible?

Q39 Mr Malik: I am going to come on to that shortly. To move on to alternatives to increased detention, the first question is for JUSTICE and then everyone can come in. You make three suggestions, in terms of alternatives to increased detention: developing the Threshold Test for prosecutors, bringing into force Part 3 of the Regulation of Investigatory Powers Act, and allowing intercept evidence. Essentially, these are procedural. Do you think they are all that is needed?

Dr Metcalfe: I would be surprised, if you lifted the current ban on intercept evidence and ensured that there was greater understanding of the Threshold Test, whether you would not diminish significantly some of the evidential or operational challenges that the police face currently, in relation to terrorism investigations. To take the last point first, intercept evidence is the most important part of that argument. It seems, from reading Andy Hayman's letter, that a great deal of the reason, or suspicion, that the police have that individuals are involved in terrorist activity comes from evidence that is obtained through intercepted communications. Were evidence of this kind made available, admissible in court, then one would imagine that the police would have much less difficulty. To talk about the other two points, the Regulation of Investigatory Powers Act of 2000, Part 3 of that legislation contains provisions whereby, if someone has an encryption key and refuses to hand it over at the request of an authorised person, they will be subject to criminal sanctions. Basically that allows for, following trial, that a person can be made subject to imprisonment. It seems to us that this was a fairly

straightforward way of cutting through the computer evidence problems which were indicated in the Metropolitan Police's letter, because they indicated that they had difficulties with obtaining encryption keys. If the person whose computer it is refuses to provide you with an encryption code then they have committed a criminal offence under Part 3 of the Act. The difficulty is, of course, that Part 3 has not been brought into force. These are powers which the Association of Chief Police Officers asked to be brought into force, in their letter of 22 July; to date, as far as we are aware, the Home Office has not done so, the Government has not done so. Turning, just very quickly, to the Threshold Test, I am not really sure that a change is needed. The words we used were 'greater clarification', because it seems to us, looking at the difficulties that are said to exist where the police do not see how they can have enough evidence to charge a person, it is very difficult to reconcile that with the text of the Threshold Test, and this is set out in a public document, the *Code for Crown Prosecutors*. What it says is that Crown Prosecutors have to decide "whether there is at least a reasonable suspicion that the suspect has committed an offence . . ." It applies to "cases in which it would not be appropriate to release a suspect on bail after charge, but the evidence to apply the Full Code Test is not yet available." In essence, what the Threshold Test is saying is, if you have a complicated, ongoing criminal investigation and you do not have all the evidence back, it is perfectly appropriate to apply the Threshold Test, where it is in the public interest, to ensure that a person is brought up on charges. As I said, this is a publicly-available document. It has not been made clear to us, in any of the debate since the July bombings, why the Threshold Test is somehow inadequate. I do not know whether this Committee is planning to take evidence from the Crown Prosecution Service but I would be extremely interested in their answer, as to their views why the Threshold Test is inadequate.

Q40 Mr Malik: To the other three witnesses. I know that already some of you, both today and previously in the public domain, have made your feelings clear on intercept evidence. Do you agree with JUSTICE's suggestions and are there any potential problems with these steps? The final question was going to be around intercept evidence and whether you would have any objection to it being brought forward as evidence in court? Do you agree with JUSTICE's suggestions, are there any potential problems with the steps that they propose?

Mr Owen: I agree with it. I cannot understand the current situation. There is certainly no human rights obstacle at all to admitting intercept evidence. Clearly, the objection has come from, I understand, solely the security services and GCHQ, who are concerned about releasing information. I think if you talk to any law enforcement agency, anywhere in the world, and tell them our approach to intercept evidence, they regard it as absurd. The five godfathers of New York crime families are all in jail at the moment, thanks to intercept evidence. The Senate review of the operation of the Patriot Act has

7 February 2006 Dr Eric Metcalfe, Ms Shami Chakrabarti, Ms Gareth Peirce and Mr Tim Owen QC

identified intercept evidence as essential in getting convictions. I do not understand it. The idea that the criminal courts at the moment do not have ways of preventing disclosure of technical aspects of the gathering and collecting of evidence in circumstances where it is not necessary to the fairness of the trial to reveal those technical issues is simply wrong. Such safeguards already exist within the public interest immunity process, which applies in all criminal trials at the moment.

Ms Chakrabarti: This has been Liberty policy for some years. It is sometimes so surprising that it makes the front page of the newspapers. We do give up some of our privacy when it is necessary and proportionate and you cannot actually think of anything more proportionate than having telephone taps to prevent terrorist outrages. We would prefer if judges issued the warrants, that would be a helpful safeguard, but if you are listening in, that is the privacy interference, why not use it in court, sometimes it might even exculpate a defender. This is a no-brainer from a human rights perspective. I understand that there are operational concerns, but really they need to be addressed, because, we just have to look at the hard reality of us being so alone in the world, the United States do it, so many other people do it, we admit their intercept in our courts, and there are issues about reciprocity. I am disappointed that this debate has not moved on further more quickly.

Q41 Mr Malik: You are at one with JUSTICE's suggestions, the three which I outlined?

Ms Chakrabarti: I think so.

Ms Peirce: If I were defending someone who was guilty, I would regard intercept as a big problem for the defence. If I were representing someone who was innocent, I would be aghast, as I am often, that we cannot have that evidence. It is obsessive secrecy on the part of the agencies which have the intercept capability, and it is madness really, frankly, for this country to go on as the one country which does not use it.

Q42 Mr Spring: Just in passing, I must say, for the record, I think it is very important that you expressed yourselves on that point so robustly, and I think there is a considerable amount of sympathy for that, in all sorts of quarters, in the House of Commons. I want to move on to the question of what happens post-charge and refer particularly to the submission from Liberty in this regard. I note that you talked about, in this whole area of re-interviewing and recharging, that you would suggest an amendment, which I thought was interesting, to allow for re-interviewing, and I quote, "in cases in which the Secretary of State considers it to be in the interests of national security or if the person is arrested in connection with terrorism." It was framed very widely. Specifically, Ms Chakrabarti, you suggest, in allowing the questioning post-charge, that there should be a widening of this Code of the Police and Criminal Evidence Act. Apart from

the possibility of abuse, which obviously we have to be sensitive about, why actually do you think this has not been adopted?

Ms Chakrabarti: It is a very good point. Maybe the practitioners will have a better insight into that. There are obvious dangers with oppressive and continual questioning, I can understand that, but just to say there are different degrees of violation of this, that there are more proportionate approaches to these difficulties that we all face, of our locking up people for extended periods without even charge. When you look at the role of judicial safeguards, there are certain concerns that I think judicial safeguards are capable of re-meeting, so if one were to go for a lot of additional questioning post-charge and one was concerned about oppression, that is the kind of moment where I think potentially a judge could really help. Where a judge cannot help to safeguard a process is where there is no process at all because there is not even a charge. Maybe, and this would be interesting to hear from the police and the CPS again, they feel that once someone has been charged there is a disinclination to speak, no real incentive to speak, because the person has already been charged. I would be very interested in their view. All of this would be far more proportionate than the alternative put by Mr Hayman.

Q43 Mr Spring: Thank you for that. I wonder if the others might wish to comment on that. You make the point about protection and there may be some judicial oversight of this, but of course the opportunity arises for new evidence to be produced, which obviously could be hugely important and beneficial to a resolution of this particular problem?

Mr Owen: From a Human Rights Convention point of view, there is a fundamental right not to incriminate yourself. It is an important principle, once you have been charged with an offence, that you are not then compelled, on pain of adverse inferences, and so on, being drawn against you from then re-interviewing you, having been charged; that is really not the difficulty that I think we are facing here. At the moment, if I am arrested for burglary and then, while I am on remand awaiting trial for burglary, the police get evidence that I may have committed a murder, they can arrest me and interview me for the different offence. What we need to consider, I think, is a scenario in which the police have initially arrested and charged with one level of terrorist offence; and then in the course of the investigation they then get other evidence which enables them to believe that a more serious terrorist offence can be charged. The question is, in those circumstances, where it is a graver offence arising out of, if you like, the same charge, what are the human rights obstacles to interviewing again post-charge? The answer is, subject to not using evidence and breaching the privilege against self-incrimination, not using compelled questioning against a suspect, there is nothing, in principle, to prevent the holding of an interview, the presenting of the fresh evidence to the suspect and questioning and inviting the suspect to give an answer to it. Having been advised of their right not to say anything, if

7 February 2006 Dr Eric Metcalfe, Ms Shami Chakrabarti, Ms Gareth Peirce and Mr Tim Owen QC

then they give answers, that evidence can be given at the trial. There is not a difficulty, in my view. Certainly there is no fundamental primary legislation or human rights principle which prevents an amendment to the Code in a way that Liberty and JUSTICE have suggested.

Dr Metcalfe: I am in complete agreement with what Shami and Tim have said. We believe that post-charge questioning is already accommodated under PACE, but for the avoidance of doubt, in terrorism cases, we would not have any objection to a suitable amendment to make this clear.

Ms Peirce: We do not have an inquisitorial system and our adversarial system is not really matched to having continuing inquisition after charge. However, certainly there are cases, which we are all familiar with, where a person has been charged, for instance, with conspiracy to cause explosions, then a lock-up has been found with explosives in it and that person has been re-arrested from prison, taken to a police station and interviewed about a different substantive offence; so it is catered for, in many ways, already.

Q44 Chairman: If I could just interject for a moment. Earlier, I think all of you were saying that there is a certain point, seven days, perhaps 14 days, and if you have been questioned for all that period of time, you begin to get to a situation where judges then would be wary about taking evidence into account. If you have post-charge questioning, it does seem to me that, from the point of view of the person being questioned, though technically you may have moved from one charge to another, it must feel awfully like you have been questioned for 14 days or more in a row. Do not the same human rights issues arise as for somebody who has been under continual questioning for a long period of time, albeit in the technical legal sense the charge in question has been changed, or am I misunderstanding it?

Mr Owen: I was responding, and I agree with Gareth Peirce's view, that there is a difference between being held continuously for seven to 14 days in police custody without any charge and then the increasing pressure that brings on any human being, and then therefore doubts about the voluntariness of any admissions which then are given. There is a difference, it seems to me, between that scenario and another scenario, whereby you have been charged. Yes, you have been remanded in custody, and living a regime, probably a horrible regime, of detention in conditions of high security, in Belmarsh Prison. But if you are asking me whether an interview, three months, six months on, on the basis of new evidence which has come to light post-charge, would be fundamentally objectionable purely because it would be oppressive, in and of itself, I do not think it would be, necessarily, no.

Q45 Mr Spring: What the Committee has been looking at obviously is what happens in other jurisdictions, particularly countries that have suffered problems with terrorism, notably France and Spain. It is my understanding that charges are laid rather more rapidly, if one can generalise, in

these countries but that the period of detention, when further questioning and interviewing take place, is a period of time considerably longer, so there is a kind of difference in balance between, again, this country and perhaps others. Do you think that the balance which exists in, say, countries like France and Spain is a more appropriate one, or not?

Ms Chakrabarti: I think one has to be careful about this extrapolation of completely different legal systems. I personally would not advocate, for all sorts of reasons, moving wholesale to an inquisitorial system of justice. I think actually that English adversarial criminal justice is the paradigm of due process and it has been adopted all over the world and forms the framework of the Convention of Human Rights. That said, you must know the charge against you. I would say that nobody wants a situation where people are detained for years and years pre-trial; that can be very oppressive and very harsh for someone who ultimately is acquitted. The test there is reasonableness and you must expedite prosecution and preparation for trial as quickly as possible, where the judge can really chivy things along, but this crucial period of being between arrest and charge must be kept to as short a period as possible. The charge is the bare minimum of the case against you, the reason why.

Q46 Mr Spring: Of course, you make that point. I think what we are talking about is post-charge, post-charge detention, which is not quite the same thing, to say the least. I think it is on that we want to have some sort of clarification. I take your point totally that legal systems are different and so are traditions, but is there some advantage, to your knowledge, of what happens in these jurisdictions from which we can draw? That is really the essence of the question.

Mr Owen: I think it is a myth, actually, I really do, and it is not being parochial. It is not that we always do it better. But the idea that other countries, before the European Court of Human Rights, get away with, if you like, some much more draconian system of post-charge detention I do think is a myth. As I say, I know of cases myself, that I have been involved in, where suspects have been on remand for up to two years before the start of their trial. The European Court of Human Rights does not set down rigid time limits for the right to trial within a reasonable time.

Ms Chakrabarti: Everyone is bound by the Convention but what it is important to say to the Committee is that the Convention, rightly, is more forgiving about lengthy detention between charge and trial than it is about lengthy detention without charge, or pre-charge.

Dr Metcalfe: It has never been suggested, in any of the debates, in relation to terrorism detention powers in this country, that somehow post-charge detention in European countries has made those countries safer. Post-charge detention exists in this country if you are refused bail, if you are seen to be a risk to public safety and the court refuses bail on that ground, then, yes, you will be held on remand until your trial. I agree with Shami and Tim again

that, the extended periods of custody that you have in European jurisdictions are nothing to be emulated and it has not been suggested anywhere in this debate that somehow post-charge detention would make the country safer, in any event.

Q47 Mr Spring: If I can ask just one final question, and I think I know what the answer is going to be, which is the alternatives to custody, for example, control orders, tagging, specific surveillance, I wonder if you would make some judgments about how efficacious that might be and how protective of the individual that might be, and what difference there might be?

Ms Chakrabarti: Control orders are a nonsense; the people who wear plastic tags in their homes, if they are so dangerous they should not be there, they should be charged and they should be detained pending trial. They are the cruelty without the benefits of security which come with incarceration. Alternatives, I think one of the things we explored is bail with conditions. The trouble with control orders is that potentially they are indefinite punishment without trial. Again, if one were really interested in more proportionate alternatives, Mr Hayman and his colleagues, or perhaps people better qualified to advise on criminal policy, might suggest bail with conditions with a hard-edged end date for trial. With regard to these two parallel systems that do not make sense, indefinite punishment without trial but is not incarceration, and therefore is not very safe, on the one hand, and then very long pre-charge periods, on the other, which amount effectively to internment, so says Lord Lloyd.

Q48 Mr Benyon: Just on that, in paragraph 14 of your submission, you talk about, this is Section 47 of the Police and Criminal Evidence Act: "Conditions could include curfew, reporting, or the surrender of a passport." Is that what you were just referring to?

Ms Chakrabarti: I am talking about that, as a bail condition, has an end point; bail is part of this criminal justice process that I have described, that begins at the point of charge.

Q49 Mr Benyon: You are talking about potentially the most dangerous people in this country?

Ms Chakrabarti: If they are so dangerous they will not be on bail, quite rightly they will be remanded in custody, which is how things work.

Dr Metcalfe: With respect, you asked us the question, what do we think of control orders as an alternative to detention. We are not saying that people who have been refused bail have been refused bail wrongly necessarily, we are simply making the point that control orders do not really show much of an alternative. In fact, they are worse, because they lack the possibility of vindication. With a control order, you are held more or less from year to year without ever having a criminal trial to clear your name, you are simply held on suspicion of the Home Secretary.

Mr Benyon: I could take it much further but I will leave it there.

Chairman: I have a couple of points about what we were told in France that I was going to raise too, but I will not, we will move on.

Q50 Mrs Dean: If we could look at the possibility of greater involvement of the judiciary, the existing procedures require judicial oversight of the more limited extensions presently available. How do you think this oversight works; is it effective or is it just a rubber-stamp of police requests?

Mr Owen: I think the relevance of this is the idea that, again, you have not got enough evidence to charge and so you are going to prolong the pre-charge detention and you are going to make it Convention-acceptable by involving a judge who will monitor the process, and that will make it compatible. The difficulty, however, it seems to me, is this, and we are back, I suspect, to the problem of intercept evidence, because either there is sufficient material, I will use the word 'material'—

Q51 Chairman: Mr Owen, if I can help, can we focus on existing practice, because at the moment judges are approving this. I think the purpose of this question is, at the moment, in your experience, is this a real process, where judges really scrutinise, or is it actually a rubber-stamping of requests?

Mr Owen: I shall have to be careful about my language. From the point of view of the defendant, or a defence barrister, attempting realistically to persuade a judge, at the point where the CPS hold all the cards, they have all the material, they can give you bits and pieces in various forms, they do not have to serve all their evidence for up to six months, effectively it is a rubber-stamp. We do not have, and this is not a criticism, a *Juge d'Instruction* model, where you have a neutral judge whose role is to investigate evidence both for and against the accused. We have a system, a separation of powers, the police and the CPS collect the evidence, they present it to a judge, who at that stage is simply saying, "Well, is it enough to justify effectively a charge and then detention pending trial?" Inevitably, they tend to say "It's enough; we'll tick the box and refuse bail."

Ms Chakrabarti: This is no slur at all on the judiciary, of whom obviously I am a great fan. Let me put it this way, and this is a bold statement indeed. Up until the point of charge there is very little that a judge, or anyone, can do to make a process fair; it becomes fair in our adversarial system at the point at which the bare minimum is put to the defendant and they can start to argue their own side of things, and therefore the judge can start seeing the alternative point of view. I would say this, forget the judges, put the Director of Liberty in charge of this process and she will become a rubber-stamp, because she will hear one very compelling side of the argument, which is, "There is secret intelligence. I know something you don't know. This person is a very dangerous suspect," and what else has she got to go on, and there is a potential terrorist atrocity. That is the problem. What makes the process fair in our system is that adversarial aspect, which cannot even begin until someone has been charged.

7 February 2006 Dr Eric Metcalfe, Ms Shami Chakrabarti, Ms Gareth Peirce and Mr Tim Owen QC

Dr Metcalfe: I agree completely with what has been said before.

Ms Peirce: I agree.

Q52 Mrs Dean: Can I turn to you, Dr Metcalfe. JUSTICE say that Lord Carlile's proposals for strengthening judicial oversight would not work because a judge does not have the training or the powers of an examining magistrate in the civil law system and because such training and powers would be incompatible with the common law system. Is it not reasonable to try to increase judicial oversight of detention?

Dr Metcalfe: I agree that more judicial oversight is always a good thing but, as previous discussion has made clear, at the pre-charge level there is actually very little for judges to scrutinise. The alternative which was suggested by Lord Carlile, first of all he proposes the introduction of a small group of security-cleared, designated, senior circuit judges, acting as examining judges. The term he uses, 'examining judges', refers of course to the continental system that you find in Spain and France, for instance, and yet, when you look at those systems in detail, the background of a judge in those jurisdictions is not typically the background of a judge that you would find, that is to say, a practitioner, in this country, someone with long experience of courtroom law. The background of a judge often will be either as a prosecutor or actually there is a separate judicial track, if you like, in the legal profession, there is almost a separate profession of judge in the administrative court systems. That is a completely different style of training, and the systems which have that type of judge are used to having their police forces controlled at the investigative stage by an examining judge. I am not sure what the police forces in this country would think about taking directions from an examining magistrate, in the way that they do in France and Spain. For all the reasons that we set out in our written evidence, we are extremely uncomfortable that the common law adversarial system that has served us so well for so many centuries is being tinkered with because of a level of police dissatisfaction with the pre-charge process. A second proposal that Lord Carlile made, a feature of the system, if you like, that we are very concerned about, is his suggestion that you could use special advocates. You will be aware, of course, of the concern over the use of special advocates in relation to the Special Immigration Appeals Commission and indefinite detention under the 2001 Act. I have to say that I find the idea of using special advocates at the pre-charge stage also very disturbing. One of the essential guarantees that you have under the European Convention on Human Rights is that someone who is subject to detention has the right of access to a court, and the right of access to a court means being able to know all the evidence that is tendered against you. With the system of special advocates, by contrast, you will be in a position whereby you are detained, someone is appointed to represent you, that person is not able to discuss with you the evidence against you, and a court proceeding

takes place in your absence. That is to say, you may never know the basis of the evidence against you and you will be in no real position to be able to challenge that.

Q53 Mrs Dean: What about the Canadian system of investigation; does that not provide a model from another common law system?

Dr Metcalfe: I discussed that with Mr Owen earlier. It is actually quite a different system and it is not at all the examining magistrate system that we have been discussing in relation to, say, France and Spain. In Canada, you have something which is modelled much more on the provisions we have in the Criminal Justice Act 1987, which establishes powers for the Serious Fraud Office to ask people a bunch of questions; in Canada the system is under the Anti-Terrorism Act 2001 and that system is controlled by a judge. Really it is an evidence-gathering mechanism and the person themselves is granted immunity: nothing that they say in relation to any of the questions that they are asked can be used against them in relation to later criminal proceedings. What the investigative judge system under the Anti-Terrorism Act in Canada is used for is to gather evidence against other people, so you call someone in, you question them and you build a case against someone else. The system in Canada allows a police officer to refer a case to a judge, the judge takes hold of the file and calls in witnesses and then builds a case on that basis. It is a tribute to what a great device this is in the Canadian system, the Attorney General in Canada is required to report annually to Parliament to tell them how the system is going and, according to the most recent report, in 2004 the sum total of requests made to courts under this power between 2003 and 2004 was zero. In fact, there has been only one case that I am aware of and that was in relation to the Air India bombing, the criminal proceedings which related to the bombing in 1985. So not exactly a great shining way forward, not necessarily to be ruled out completely but I cannot see a great deal of enthusiasm for it.

Mr Owen: Just following on from that, I think Lord Carlile bases his suggestion on what was in the Newton Committee's Report. I do think that there is a misunderstanding about how the Canadian system operates, and I agree with what Eric Metcalfe has just said. It seems to be believed that under the Canadian system you can have a special disclosure judge, if you like, who sits in camera with the prosecution, no defence in, and the prosecutor and the judge then prepare a sanitised version of otherwise sensitive evidence, and that this evidence emerges to be presented to the defence and before the jury in a way which the defence can never go behind, therefore they are not able to challenge the sanitised version. That is just not true; that is not how the Canadian systems work, and Eric Metcalfe's analysis is right. The Canadians would never seek to have a situation where important evidence is introduced in a criminal trial without the ability to challenge it. Of course there are ways, and I have referred to it in terms of the public interest immunity certificate, which means that you do not

have to disclose everything about how you are gathering your evidence, unless it is regarded as essential for a fair trial, and in many cases it will not be. I do think that, in your further investigation, you may want to get evidence from a Canadian lawyer or somebody with real experience of it, but my understanding is that this cannot really provide us with much assistance.

Chairman: Thank you very much indeed.

Q54 Mr Benyon: I want to look now at some of the practical difficulties, in terms of the timescale concerned, and I suspect the majority will be towards you, Gareth, but others may wish to chip in. I read your article in the *Guardian* and one thing that comes straight out of it is the constraints at Paddington Green. I think we had all rather hoped, or assumed, that the large amount of money which had been spent there had made at least a practical building, if not a particularly comfortable one. If we can work through various of the points which you have raised and which Lord Carlile has raised and his concerns about this as well and start with the question of interpreters, the police argue that the need to find interpreters causes delays. In your experience, what proportion of cases involves the use of interpreters in questioning suspects, and are the languages that they are required to interpret on rare, or are they readily accessible?

Ms Peirce: The category of case that is being considered in this discussion involves particular suspects. Although July 7, which triggered this debate, was British young men and many people detained at the present time are British young men, on the whole there have been many arrests and detentions in the past five years in which the language has been universally Arabic. No shortage of Arabic interpreters. I have never heard of a shortage of Arabic interpreters, there are always sufficient Arabic interpreters at the police station.

Q55 Mr Benyon: Would you suspect that there has been a delay in questioning a suspect or a delay in you having access to a client on the basis that no-one could find an interpreter?

Ms Peirce: I am sure not, because it is mandatory, when a person is brought in, that their name will be taken, basic details, and the custody record will be gone through, that they will be told their rights to finger-printing or DNA samples; they have to have an interpreter there. I have no experience of that difficulty at all.

Q56 Mr Benyon: When cases come to court, there is no difficulty in putting forward evidence on the basis that there was not a proper interpreter at the time?

Mr Owen: I have had no difficulty with that. It slows the trial down, having an interpreter, but that is all.

Q57 Mr Benyon: This is really to everybody. The police claim that greater resources will not solve their problems, and the quote that we have been given is: "the process of staged disclosure to the defence, consultation with clients to take instructions, interview and assessment is essentially

sequential." How far do you agree with the police that greater resources will not solve their problems in this respect?

Ms Chakrabarti: That is an assertion which makes no sense to me whatsoever. A lot of what they say, "We have difficulty getting material from this country or that country, we have difficulty getting forensics back," if you were to have, for example, a number of atrocities in different parts of the country you would have to—all of those points are put and surely they beg for more resources. Also, of course, they predicate the whole argument on the basis that the investigatory clock begins ticking almost only at the moment of arrest. Clearly, that is not true and should not be true, and the investigation can only be improved, it would seem to me, by more and better qualified resources. I am afraid, as so often in this document, there are sweeping assertions that are not borne out, and that, I am afraid, "resources won't do the trick" seems to be something that is added possibly when Liberty, or someone else, has popped up on the TV and said "Spend the ID card budget on resources."

Ms Peirce: The Anti-Terrorist Squad has its own methodology and it is one at which one expresses extreme frustration, for 48 or 96 hours, saying, "Come on, come on, if you're going to interview, let us know what you're going to interview about, let's get on with it, let's have some interviews; the person I'm representing wants to know why he's been arrested." The police say, "We are only going to go at our own pace, and we have the way we approach it and we can't go any differently." Individual interviewing officers say, "It may be crazy but this is the way we're doing it." It may be 48 hours before a person is even being asked where he was born, where his parents are living, all of that; it is frustration, from the point of view of the detainee, in terms of how it progresses.

Q58 Mr Benyon: They might point that frustration towards having to put a trial before a very clever QC who may expose them if they do not follow the procedures absolutely to the letter? I am being devil's advocate here.

Ms Peirce: I think, unlike the job of a QC, the job of a solicitor in a police station is to protect the interests of the person you are representing, but also to have some sufficient flow of information that the person knows why he is there, it is a fundamental right. You could be there on suspicion of involvement in, the term is, 'commission, instigation, preparation of acts of terrorism', that is the catch-all phrase in the legislation that is used to arrest and detain people, and you may know nothing more than that phrase for the whole period of time you are in the police station. If there is a grudging process of disclosure, over seven days or 14 days, you may still not know at the end.

Q59 Mr Benyon: They say there is another problem, which they also allude to, in the case study that is in your paper, that the delay is caused by one firm of solicitors representing most of their suspects. What would you say about that?

7 February 2006 Dr Eric Metcalfe, Ms Shami Chakrabarti, Ms Gareth Peirce and Mr Tim Owen QC

Ms Peirce: I am not sure if that is apocryphal. I am aware of one case where one firm acted, I think, for the majority, not all, of the detainees. I know of this indirectly, not directly. Certainly, I would say, the only professional way in which you could represent people would be if you had the manpower, or womanpower, to do it. Certainly, speaking from my experience, in our firm, if we were asked to act for more than one person, we would only do so, and could only do so, if we were able to act responsibly for that person. I am not at all sure. I find this a very dubious proposition. It would be appropriate for the police, if a solicitor was representing more than one person and could not deal with it, to say, "I'm very sorry but we're going to have to explain to the person you represent that they can't be interviewed properly because you can't do it." If it is the example I am thinking of, I am sure that firm did have a very large number of people available. I cannot say more than that, but I am very dubious about the legitimacy of that example given by the police.

Q60 Chairman: Just out of interest, can I ask how many firms of solicitors, or perhaps how many individual solicitors, would you say have some specialism in this area of law?

Ms Peirce: I think, probably more than I would know, in the sense, there is a duty solicitor scheme and I would have thought at least half, and probably more, I am only guessing, of people detained under any terrorism legislation would ask for the duty solicitor, would not know a solicitor. However, rather like the case of the Irish community, as it becomes more the position that it is a suspect community, in a sense, so the Muslim community in this country is aware that it is a suspect community and people who have no reason to worry about the law begin to think they ought to have a solicitor's number, and their families do. You get to a position where if someone is arrested people in that community will be ringing each other to know if there is someone who has some relevant experience. I would have thought there is a reasonable number of firms which are within that range of familiarity, in the most general terms, but they are not necessarily firms that will be called in the police station. If a person asks for a duty solicitor and there is a solicitor in place, even if the family have asked subsequently for a named solicitor, that solicitor will already be embedded, so to speak, in the police station, the duty solicitor, and will continue with the interviews.

Q61 Gwyn Prosser: Ms Chakrabarti, in cases where a detainee has chosen one specific solicitor and that person is not always available, you have made a tentative suggestion that there might be scope for stopping the clock. How practical would that be and how could we avoid even that process being described as an abuse?

Ms Chakrabarti: Actually, I have been rather heartened by Ms Peirce's practical insight. Remember, of course, that I do not spend time in Paddington Green, not yet, until new speech offences put me there, but at the moment I am not in

Paddington Green. If I am detained in Paddington Green, I am probably going to 'phone Ms Peirce or Ms Christian. Ms Peirce was saying that solicitors have professional obligations and if they cannot meet them, and the fact that they are going to act in this interesting case means it is almost going to be floundering in custody, unrepresented, then they should not represent them. You see already, just through professional ethics, a much more proportionate response to the idea that you have to lock people up for longer periods because everybody wants to be represented by whoever it happens to be. In my case, probably it would be Ms Peirce. I do not even wholeheartedly support this suggestion. We mentioned this clock-stopping scenario just to highlight the fact that we approach this in good faith and the police dossier does not even explore any more proportionate alternative to the problems that they raise within this extended detention. I think there would be real difficulties with scenarios where the clock stopped because you insisted on Ms Peirce, and it would require a great deal of safeguard, but it would certainly be more proportionate than what ended up being the police proposal. I think Ms Peirce gave the best answer. If a firm cannot provide the representation, if an individual celebrity solicitor cannot do all the work, they have professional obligations to say so.

Ms Peirce: There are occasions when there is more than one person in a police station asking if a particular firm can represent them, and they or their families think that is the guarantee that they will be represented correctly. If you cannot, sometimes you will talk to that person and say, "I cannot. There are three solicitors, we are able to go to the police station, we cannot represent a fourth person," over however many days it can be, "we cannot do it; but I would be very happy to give you the names of two or three firms which I think have relevant experience." I do that, I do that often, and I do it not just in London but people could ring from a police station in Liverpool or Manchester and I would say, "This is who I suggest you might have." I do not accept this police example which is given.

Q62 Gwyn Prosser: Ms Peirce, you have told us this afternoon that very often there is no interview or proper contact for the first 48 hours, and then when the interview starts it is very perfunctory, it is "What's your name; where do you come from?" etc. You have given us that, in anecdotal terms, of course. How precise can you be? What proportion of cases that you see, for instance, in Paddington Green Police Station, follows that pattern?

Ms Peirce: Over 25 years, or whatever, I would say 90% of the interviews have followed that particular pattern. If it is of assistance to the Committee, I will try, within my office, to go back and take perhaps 10 sample cases and try to quantify it more particularly; but that is a pattern, the police will tell you they have that methodology, I am sure.

Q63 Chairman: That would be enormously helpful, if you could do that, and could you expand a little in your search, I think you have just touched on the

7 February 2006 Dr Eric Metcalfe, Ms Shami Chakrabarti, Ms Gareth Peirce and Mr Tim Owen QC

same point, that this appears to be part of the deliberate approach of the counter-terrorist section of the police?

Ms Peirce: Indeed; yes.

Q64 Chairman: Have you explored with them at any time why they adopt this approach, which now, in other cases, they are citing as evidence for needing more detention?

Ms Peirce: Although part of the rationale is, if you have 10 people in custody, it is rare that it is that number, that perhaps if there is a suspicion that they want to progress in unison through the interviews to compare answers, but I do not think it is that. I do not know, is the answer. They have not ever given me an answer that is satisfactory. You could go 100% quicker with all of the basic questions than they do.

Q65 Chairman: Over the time that you have been practising, the period of detention without charge has been extended. Is it your sense that this fallow period, before anything is done, has grown as the maximum period of extension has been increased, or has it always been there, even when the ability to detain without charge was much shorter?

Ms Peirce: It has always been there. May I give you just one comment on the ricin case, since Mr Hayman has referred to it. I will try to do an exact analysis of all the people detained within that inquiry, but that was a seven-day period still, it had not gone to 14 days, and, for those individuals who were represented, who were not always arrested at the same time, over a certain period, it was less than seven days that was used before charging. This is why I find it not convincing to say ricin is an example where you need 28 or 90 days; they did not use even the seven days. Two people charged with that case, both of whom were acquitted, were never interviewed in relation to the ricin conspiracy; they were charged with it, they were already in prison charged with a different offence, and they were never interviewed, they were simply charged with ricin, never interviewed. This was a point which was made to the judges, made to the jury; absolutely extraordinary that was the case.

Q66 Mr Winnick: That was covered in your article, was it not, Ms Peirce, ricin?

Ms Peirce: Not quite. I was referring to the claim that the case was lost basically because the main suspect was bailed. However, that suspect was bailed after a day and a half in the police station and it was not the first time he had been arrested and bailed within the same time period. It was no justification for extended detention.

Q67 Gwyn Prosser: On the same theme, of the use of time at Paddington Green Police Station, you have made the assertion that up to 90% of the time a person is in custody is not used in any sort of productive interviewing, so, in a 14-day detention, less than a day and a half perhaps actually is interviewing. Can you give us evidence for that assertion, when you write to us about the other matters?

Ms Peirce: Yes. I think what might be of use to you is if I give you a sample custody record, with the name taken out, so that you can see for yourselves the periods of time.

Gwyn Prosser: That will be very helpful. Thank you very much.

Q68 Chairman: That will be very, very helpful indeed; thank you. Just a few last questions. The problem with only two interview rooms at Paddington Green.

Ms Peirce: They seemed to have another one, the last time I went.

Chairman: There are now three.

Mr Winnick: They knew you were going to give evidence today.

Q69 Chairman: Do you have any sense—and this may be not an easy question, of course—of how many need to be available at least to cover 90% of the situations which arise, so that the interview rooms themselves would not be a delay, with this picture of the Edgware Road being full of lawyers drinking coffee which you paint in your submission?

Ms Peirce: I do not know. I think there are occasions when there are a lot of detainees, but even if there are, say, five at a time it is not a good place, for a range of reasons. They have used a room where a solicitor could have a conference with their client, apart from interview, for an interrogation room, so to speak, with a video, so it is robbing Peter to pay Paul. I think the police would tell you, who work there, that they find it a very bad working environment. They do not like being there for seven or 14 days. Those who are interviewing, it is not good; the interpreters are in poor conditions. If it were possible, in your inquiry, to go to Paddington Green and go into one of the cells and just see; there is no natural light, no proper heating, no proper ventilation, and it is a bad environment for seven days.

Q70 Chairman: Can I ask each of the witnesses to concentrate, if you could, just on this specific point of practical issues that have arisen in the course of questions; are there any others that you would like to stress to the Committee that we have not touched on already this afternoon, or have we covered the main, practical, organisational questions that have arisen?

Mr Owen: I think so, yes. I have got nothing to add.

Ms Peirce: No; thank you very much.

Dr Metcalfe: No.

Ms Chakrabarti: No.

Q71 Chairman: One final question, just to put to you a point that Lord Carlile has made. He argued, in fact, actually in support of your position, he said that delays in interviewing suspects are not a justification for extending pre-charge detention, because he said that most suspects will exercise their right to silence. Is that a true observation, in your experience? I do not think he defined what 'most' was. Do a significant number of suspects exercise the right to silence, or is that more unusual?

7 February 2006 Dr Eric Metcalfe, Ms Shami Chakrabarti, Ms Gareth Peirce and Mr Tim Owen QC

Ms Peirce: Probably a significant number are advised to, in part because you do not know what it is the person is there for, and therefore you are struggling. You say, "I don't think you should launch into answering questions," particularly if you have concerns that the person you are representing is not necessarily very articulate, may not be completely understanding of what is going on, or may be very frightened. You say, "Please, let's just wait until we find out why you've been arrested," which could be days along the line, "and then we can sensibly say is there something you should be answering." The wastage of time, in fact, before you know what you are there for, probably is a factor in prolonging "no comment" situations. The sooner you knew, the sooner you and your lawyer could decide whether it would be appropriate for you to answer, but then the longer the time goes on the more exhausted the detainee gets and is less able to answer questions to do justice to themselves.

Chairman: Thank you. That is very helpful.

Q72 Mr Winnick: To pick up just one comment that you made, Ms Peirce. You referred a few moments ago to a "suspect community," referring obviously to the Muslim community. I am not suggesting you were making implications against the police, but would it not be the case that when the IRA were committing their atrocities on the mainland it would have been rather foolish, to say the least, for the police to be looking into the Muslim community for the culprit? If that were the case, as obviously it would be, because they knew who were responsible, as an organisation, surely now, since ceasefire by the IRA and bearing in mind the suicides attacks of July 7, does it not make sense for the police to be looking for the obvious people within the Muslim community, however unrepresentative those people are, as we know they

are, of the vast majority of Muslims living in Britain, who are no less lawful and law-abiding than ourselves?

Ms Peirce: My comment was not directed to the police, it was in answer to a question as to whether certain firms of solicitors' names were circulated.

Q73 Mr Winnick: I understand that, but then you used that term and I am just trying to get an explanation from you?

Ms Peirce: I have to say that my experience is identical, in terms of the innocent, wider community and its apprehensions. What was the Irish community with apprehensions now has become the Muslim community in this country and people have a real fear that they could be arrested when they have done nothing wrong.

Q74 Mr Winnick: I understand that and that the Irish community, again, the overwhelming majority, like the Muslim community, perfectly law-abiding, had nothing to do with the mass murderers, and it is important, as you say, to bear in mind, which both you and I agree on. Inevitably though when you are looking at suicide bombings and those who want to commit such further atrocities then the police have no alternative but to look within that community for those who are carrying out the attacks which occur?

Ms Peirce: I think, just my own comment, having represented individuals in the Muslim community since 1997, before British young Muslims became a suspect community, a huge number of individuals in the refugee community became apprehensive that they were suspects for terrorism, and were not. That was not a happy progression of suspicion and I think led to a number of real, real difficulties in our criminal justice system.

Chairman: Thank you very much. I think that is a good point on which to end. Can I thank all four of you very much indeed; you have got the inquiry off to a good start and raised a number of issues that we will want to put to other witnesses in the subsequent sessions. Thank you very much indeed.

Tuesday 14 February 2006

Members present:

Mr John Denham, in the Chair

Mr James Clappison
Mrs Ann Cryer
Mrs Janet Dean
Nick Harvey
Steve McCabe

Mr Shahid Malik
Gwyn Prosser
Mr Richard Spring
Mr Gary Streeter
Mr David Winnick

Witness: **Lord Carlile of Berriew QC**, a Member of the House of Lords, the independent reviewer of terrorism legislation, gave evidence.

Q75 Chairman: Lord Carlile, thank you very much indeed for joining us. As you know, this is the second evidence session in our inquiry into the detention powers. We decided to have the inquiry because of the extent of the parliamentary controversy about this issue of the Terrorism Bill and in the knowledge that the Government was likely to return to terrorism legislation in the next 18 months. Of course yesterday we had the Chancellor of the Exchequer backing an extension for the 28 days which is currently going through the system, so it is basically quite a live issue for the Committee and we are very grateful to you for joining us for this session to share your knowledge in this area. Can I start with a fairly general question. You have in the past criticised the level of public information which has been made available about the proposed extension of pre-charge detention and also the failure to explain exactly what the problem was that was being tackled. How do you think the issues could have been explained better both in terms of the problem to be tackled and the justification for the powers?

Lord Carlile of Berriew: I will give you an example to start with, if I may. Recently I produced my first report on control orders. In an appendix to that report, I reproduced, and this was not opposed, but I reproduced the control order that is imposed on most of the “controllees”, as I call them, and that enabled you, parliamentarians, and the public at large to see the extent of the restrictions placed on people who are subject to control orders, something which had not been in the public domain before. The extent of the restrictions could tell the public two things, possibly in the alternative, possibly conjunctively: that the people who are controlled are dangerous to the extent that those controls are required; and/or that the extent of the controls is so great that they come to the very limit of restrictions on human rights. Now, I think it is legitimate to have that debate from the proper level of public information as to what the restrictions are. I believe the same applies across the board on these issues. The Government should give the public as much information as they can without compromising public safety. I think this is one of the few things in the area of terrorism legislation that the Americans are better at than us. I hasten to add that I think that their legislation, the Patriot Act, for example, would never have got through the

two Houses of this Parliament and it probably would have brought a government down, but, in terms of public information, they give much more.

Q76 Chairman: That is a very helpful reply. You indicate that, in relation to control orders, more information could be made available to the public. What would you have liked to see the Government say about the nature of the problem that led to the call for increased pre-charge detention? What sort of information about the problem that was trying to be tackled could have been made available, in your view, and was not?

Lord Carlile of Berriew: I would like the Government to say more about the nature of the terrorist threat. The information is actually available in the public domain; you just have to know where to go and look for it. I would prefer it if the Government made it a little more accessible and perhaps I can give you an example. If you look at what is generally called the “first generic judgment” of the Special Immigration Appeals Commission in what had become known as the ‘Belmarsh cases’, you would see there a fairly encyclopaedic description by a judge, by a High Court judge, of the nature of al-Qaeda and its connected organisations at the time that judgment was given. Journalists on the whole, if those present will forgive me, are rather lazy and they like to have stories written for them, by and large, and do not like to look in rather dense resources, like the judgment of Mr Justice Collins there. I would like to see the Government simplify that kind of information because it is a very long judgment, by putting it in the public domain so that people understand the complexity and, therefore, often impenetrability of the terrorism threat.

Q77 Chairman: Would it be too much to ask you, for the purposes of this Committee, to give two or three further details about the sorts of issues which you understand, the sort of factual issues which you understand which you suspect the public are not aware of or do not appreciate?

Lord Carlile of Berriew: I could select, for example, as I mentioned earlier, the complexity of al-Qaeda which is not an organisation, as I understand it, in the same terms as, say, the Provisional IRA; rather, it is a loose co-fraternity of people with similar political and terrorism interests, so that would be

14 February 2006 Lord Carlile of Berriew QC

one example and I think more should be said about that. Another example, and this is getting into a sensitive area, is the issue of the way in which imams are allowed to enter this country and take up posts in mosques around the country. There are some wonderful imams in this country, I have met a few of them, but very little has been done in the past to look in any detail, I believe, into the past history of imams who have gone into some cities. The good imams do not want the bad imams anyway. There is an issue here which needs to be discussed. I would give you two more examples very briefly. One is the radicalisation mainly of young men in universities. If you talk particularly to young female students in the larger, and perhaps more rackets universities, you will find that there is a degree of concern expressed about some societies in those universities from which women are usually excluded and where there might be Islamic radicalisation. The final example I would give is the issue of radicalisation in custodial settings. Richard Reed, the shoe-bomber, appears to be somebody who was radicalised in a custodial setting. I can only give you anecdotes on that, but I have received anecdotal evidence from governor grades that this is occurring and that it is a worry to them. I do not want to exaggerate the problem, but there certainly is an issue in that context.

Q78 Chairman: That last point in fact is one that this Committee drew attention to in a report produced nearly a year ago now based on our study of what had been happening in France and the Netherlands, so the Committee is certainly familiar with that. If I understand what you say, Lord Carlile, when it comes to explaining the nature of the problem, what you are really talking about here is actually having a much higher level of public understanding about the nature of the terrorist threat as a whole, if that is right. What do you think could have been done in general to explain the case for increased detention more directly? Clearly one can understand the terrorist threat does not necessarily lead to the argument for increased pre-charge detention, so what could have been done by the Government to make that case more clearly?

Lord Carlile of Berriew: The Government, I think, has learnt the lesson of what it did not do, but should have done, by announcing that the new Terrorism Bill, whenever it appears, the consolidating and amending Bill that Charles Clarke announced, will go to a scrutiny committee. I believe that a lot more would have been achieved if the current Bill, as was the original intention, but later withdrawn, had been placed before a scrutiny committee. As it happens, I chaired the joint scrutiny committee, and there was at least one person here who was a member of that committee, on the draft Mental Health Bill. The result of the evidential process of that committee has been positive in legislative terms in that we do not yet have a Mental Health Bill, so somebody is thinking about the findings that the Committee made. I believe that an evidential process would have been

more successful than the political process and may, for example, have amended the views of highly respected parliamentarians, like Mr Winnick, if I may say so, who took an entirely understandable approach in parliamentary terms, in House of Commons terms, to the way the Bill was presented.

Q79 Chairman: Mr Winnick will have his go in a moment.

Lord Carlile of Berriew: I thought he might!

Q80 Chairman: If I can look at one further question, which is to look at pre-charge detention itself, we had a session last week with Liberty, JUSTICE and similar organisations and much of the discussion was very much on the assumption, the underlying assumption, that the purpose of pre-charge detention was to enable interviewing and questioning to continue. It is fairly clear from your remarks that actually you think that is largely irrelevant because suspects will probably be well-advised to remain silent. If the purpose of pre-charge detention is not actually to enable you to question the suspects, what is the purpose and what is the justification for it?

Lord Carlile of Berriew: As the Committee knows, I am still a practising advocate. I doubt if there are many advocates in this country or solicitors who would ever advise a suspect in custody at Paddington Green to answer questions unless they wanted to co-operate with the authorities for what we will loosely call “plea-bargaining” purposes, to reduce their sentence or to try and obtain immunity or something of that kind. The reason for that is that you have to measure—and this is something I am often asked to do though not in terrorism cases because I do not appear in terrorism cases for obvious reasons—but in other cases I am often asked to measure the damage done as between answering questions on the basis of carefully managed disclosure by the police, which could get suspects into an awful lot of trouble later if he tells lies about an aspect, on the one hand, and the adverse inference direction that is given if you do not answer questions, on the other. Most of us involved in serious cases would say that the adverse inference direction is a flea bite compared with the danger, the risk or hostage to fortune of answering questions. So, in my view, the interviewing process is actually becoming not entirely irrelevant, but near to irrelevant. To turn to the second part of your question, Chairman, the purpose of the detention period in terrorism cases, first of all, is to ensure that the act is not perpetrated, the conspiracy is not brought to fruition and, secondly, to enable the orderly gathering of evidence in order that a prosecution can be brought. But it should not be any old prosecution. It is actually, I think, in the public interest for people to be prosecuted and convicted of what they have done. I am not a believer in arresting people for shoplifting in order to get the evidence to prosecute them for murder. I believe that it should be a proper process and a fair process aimed at what is believed to be the incident, the crime. In terrorism cases, there are

14 February 2006 Lord Carlile of Berriew QC

reasons for arresting very early, they are too obvious to state, I suspect, to one of the members of this Committee. Therefore I think that a period when police and others can gather evidence while a suspect is detained is potentially very valuable. However, I do think that the 90 days argument was very badly managed because it started from the wrong end of the spectrum. If you look at the proposals that I made in my report in which quite independently, the police did not suggest 90 days to me, I suggested a 90-day maximum, it actually started with a raft of judicial control and rights to ensure day-by-day management of the period when the person was detained with a view to it being brought to an end at the first sensible opportunity.

Q81 Chairman: The point that we were being put by last week's witnesses would be: how could you possibly be sure enough that somebody should be locked up to prevent them committing a crime when you have too little evidence to charge them with anything at all?

Lord Carlile of Berriew: Well, I do not know of any case in which people have been detained without the evidence of reasonable suspicion that justifies an arrest, though I am not saying I have looked at every case that has gone to Paddington Green. There are some cases, including a couple that I am afraid are still in the pipeline, still *sub judice*, where I believe that very early arrest was absolutely necessary and the current legislation may have had an effect on the gathering of evidence. I think the Committee will have my meaning without my going into too much detail.

Q82 Mr Winnick: No one in this room or indeed in the House of Commons any more than in the House of Lords for one moment underestimates the terrorist danger facing our country, so we have got common ground. I want to ask you one or two questions and, if the Chairman will allow it, perhaps I can just go back for a moment to the clerics. We have the very welcome seven-year sentence last week of a particular person. He mentioned various clerics who had come to this country and there is no doubt that there is a very strong feeling which clearly you share that some of them at least are involved in, and you implied as such, inciting hate, if I can put it in that way. Do you think it is possible for you to give any sort of estimated number? Are we talking of very large numbers? Are we talking about a handful of extremists who have not yet been, if you like, expelled by the congregation involved?

Lord Carlile of Berriew: I could not give you examples, though there may be others here who are better able to give the numbers, but a small number can have a disproportionate effect if they are in the wrong place. If I had to guess, I would be amazed if there were more than 20 such clerics in the country, but that is a pure guess, or an impure guess, just a guess. My worry is that they are in places where there are a large number, cities and occasionally custodial institutions, places where there are larger numbers than elsewhere, of

impressionable young males. Those of us who are interested in politics remember our teenage years in which we had some very radical ideas. I remember arguing communism at the end of my parents' bed when I was a teenager. If this cannot be properly controlled in a proper debating environment where all sides of the argument are shown, it is a dangerous business.

Q83 Mr Winnick: Forgetting for the moment our teenage roots and politics and avoiding self-incrimination, perhaps we can carry on. In your paper, Lord Carlile, at page 18, paragraph 61, you say, "I am satisfied beyond doubt that there have been situations in which significant conspiracies to commit terrorist acts have gone unprosecuted as a result of the time limitations placed on the control authorities following arrest". That is a pretty serious statement to make. What evidence do you have?

Lord Carlile of Berriew: In carrying out my role as independent reviewer, I go around the country and I talk to various organisations, including the police and other control authorities. That particular passage was especially based on information I was given by a police force, not the Metropolitan Police, relating to a number of suspects—and I cannot remember the exact number, but at least eight. I did a lot of reading into this subject because I was provided with a considerable amount of material and I was satisfied that that was the case. I have also had general descriptions of such events given to me by police officers in particular, including the Metropolitan Police, but that was principally founded on something outside the London area.

Q84 Mr Winnick: If we take the mass murders of 7/7, there was no way in which they were suspected in any way by the police, am I not right?

Lord Carlile of Berriew: There is absolutely no way in which they were suspected by the police.

Q85 Mr Winnick: So it would not have made any difference whether it was 28 days or 90 days or five years—they would not have been apprehended and those mass murders would have been carried out as they were?

Lord Carlile of Berriew: That instance was an illustration of a quite different problem, the problem we have been discussing in a way earlier, which is the radicalisation of young, indigenous males. These were British men.

Q86 Mr Winnick: So the most terrible mass murder which had been committed for a very long time in this country would have taken place quite regardless of the 28 days or the 90 days and so on? You accept that?

Lord Carlile of Berriew: Of course I accept that, but, and there is a "but" here, I believe there have been other potential mass murders which have been prevented by arrests and, as you quoted, there is at least one very significant set of instances, as I would call it, in which I believe that, although an incident

14 February 2006 Lord Carlile of Berriew QC

or incidents were prevented by the arrests, it was not possible, for various reasons, to prosecute the persons concerned.

Q87 Mr Winnick: But, you see, if we take what you have said and which I have quoted, that people have been released because of the time limit, one would, therefore, expect that those conspiracies would have actually resulted in murder.

Lord Carlile of Berriew: No, because, and the same used to happen with the IRA, if people are arrested and thereby their conspiracy is disrupted, it is pretty rare for that conspiracy to be resumed. Only an idiot would start to resume their conspiracy because they will know perfectly well that their every move is likely to be watched. It may not be watched, but it is a reasonable suspicion, is it not, that you are going to be watched if you are released?

Q88 Mr Winnick: So clearly, if that is the case, Lord Carlile, the 14 days were sufficient because, as you say, they were placed under detention for 14 days—

Lord Carlile of Berriew: No, it was not sufficient because in that instance, and this is a set of circumstances crossing the Anglo-Scottish border, I have been told, and it is not just that I was told because I have seen quite a lot of documentation, and there was a review carried out internally in the police force concerned mainly with what had happened in the case, I have been told that there were people who ought to have been prosecuted about whom it was expected that they could be prosecuted if it had been possible to have enough time to gather the evidence while they were in custody. I know you are going to hear evidence later about computer encryption and that kind of thing, and I am not an expert on it, but all I can tell you is that the police say, and this is around the country, that it is formidably difficult to collect evidence during a short period while people are in custody when you have nipped a conspiracy when it is really only just in bud.

Q89 Mr Winnick: That may be an explanation for the fact that no one has been released under the complaint and not charged because obviously they have to be charged, but, of the large numbers of people who have been released, no one, once released, was later charged with terrorist offences?

Lord Carlile of Berriew: No, that is right, but there is a lot of overkill in this area because the police obviously have got to act more or less immediately on reasonable suspicion. Reasonable suspicion may be based on inaccurate information, but, if the police are given inaccurate information, that gives them a reasonable suspicion that there may be a terrorism act and they have got to do something about it. You are bound to have more arrests without what the police might regard as a result in this area than in most areas of crime.

Q90 Mr Winnick: You describe the three months' post-charge detention as a "reasonable maximum", and you would clearly choose this period, and you were often quoted in the debates understandably by the Government and their supporters on this issue, rather than 28 days.

Lord Carlile of Berriew: Yes.

Q91 Mr Winnick: So why three months? Why not six months? Why not nine months?

Lord Carlile of Berriew: It is a very difficult question to answer and the answer runs like this: nobody has suggested to me that 90 days was appropriate, but I have, as I said earlier, spoken to a lot of groups, the police and others, including of course some other people who gave evidence before you insofar as they were willing to talk to me, over a long period of time, and I have been doing this now for over four years. I believe that there would never be an instance of more than about three months in which the police could not gather enough evidence if the evidence was available. I believe that there are only maybe a couple of cases every two or three years, and you might have a flurry of them and then have none for three years, in which it would be necessary to hold anyone for anything like up to three months. It was simply a judgment that I made. Six months, I would have said, was outrageous and 28 days, I think, was too little, but that is a judgment. Of course I emphasise, as I keep emphasising, that what I said was that we should introduce a new system which was consistent with the recommendations of the Newton Committee, a system that involved taking a senior judge and effectively making that senior judge something like a *juge d'instruction*, but better. The *juges d'instruction* are not judges, in my view, but they are basically very skilled prosecutors. I thought that, if we introduced a senior judge, a senior circuit judge with great experience of crime who would be there, on hand, with special advocates available to look at all the evidence on a day-by-day basis, we would probably get most people being released after, at the most, 14 days, but the judge would be there, giving reasons to examine all the material and could ensure that this was a fair procedure.

Q92 Mr Winnick: Parliament increased the seven days to 14 days, as you know obviously, less than two years ago.

Lord Carlile of Berriew: Yes.

Q93 Mr Winnick: Therefore, do you believe it is justified to jump, having doubled the period in less than two years, from seven to 14 days? Do you, Lord Carlile, a distinguished lawyer as well as parliamentarian, consider it perfectly justified to go in one jump from 14 days to three months?

Lord Carlile of Berriew: As long as a whole new raft of protections is introduced far and away beyond anything available for the 14 days to ensure that nobody is kept in for a day longer than is necessary. I actually believe that the Government was moderately sympathetic, perhaps more than

14 February 2006 Lord Carlile of Berriew QC

moderately sympathetic, to the way in which I presented it, but it was thought it was perhaps too complicated to introduce it now. I do think, and I have said this publicly, that the management of the current Bill has not been particularly skilled, it did not need to be done in such a hurry, and I would have preferred an evidential legislative process, the sort of thing you are doing now.

Q94 Mr Winnick: Lord Carlile, no one would exaggerate this, and certainly most of us have avoided doing so, by saying that three months is more or less what happened with the IRA and the Loyalists over internment, and obviously there is a difference. However, bearing in mind what you said earlier both to the Chair and to myself about extremists in the Muslim community, do you at all accept the argument that, if it was three months, the danger would be one of antagonising large elements of the Muslim community where people would be held for a maximum of three months, and I accept that it would be less in many instances, and then released in large numbers, like under the 14 days, without being charged, and would that not play right into the hands of the people that you and I recognise are very dangerous to the Muslim community as well as to the wider community in our country who would say in effect, "This is how Muslims are being treated"? Do you recognise the acute danger of playing right into the hands of those extremists?

Lord Carlile of Berriew: Of course I recognise the point. I believe—

Q95 Mr Winnick: A strong point?

Lord Carlile of Berriew: Perhaps I could just finish. I believe that the Muslim community is extremely responsible and I believe that there are large elements of the Muslim community who are very keen that there should be a full raft of powers in place that ensure that the Muslim community is not subjected to the sort of criticism that is sometimes levelled at them. Let us not forget, we happen to be talking at the moment about Jihadists, but the last major lot of terrorism we had in this country was absolutely nothing to do with the Muslim community at all and it was connected with the island of Ireland. One of my concerns, and I think Mr Clarke now has this very much in mind, indeed I know he has had it in mind since he first became Home Secretary, is that we should have some permanent terrorism legislation that will stick and be reliable against all potential forms of terrorism which we cannot predict in the future and should hopefully last as long as the Offences Against the Person Act of 1861.

Q96 Mr Winnick: Could you name anyone from the Muslim community who has come out in favour of the three months' proposed detention which you advocate?

Lord Carlile of Berriew: No, I could not name any individual, but I did not have notice of the question and I might have been able to if I had done.

Q97 Mr Winnick: But you cannot name any?

Lord Carlile of Berriew: I cannot off the top of my head, no.

Q98 Mr Streeter: Lord Carlile, I have got some specific questions about alternatives to detention based on evidence from witnesses to date, but just picking up the specific example you have given of cases where a longer period would have enabled the police to prosecute rather than release, I do not recall the Government arguing that in the run-up to this Bill going through Parliament. We were crying out for specific examples where the 90 days would have been helpful and I do not recall them coming up with any examples, albeit anonymous examples, at all. I know you do not speak for the Government, but can you comment on that?

Lord Carlile of Berriew: I thought that the Government, and I think ministers occasionally, have cited what I have said to what Mr Winnick read out. It is very difficult to cite examples in this area because it involves revealing quite a lot of information about cases.

Q99 Mr Streeter: But you have just done it.

Lord Carlile of Berriew: Well, to a limited extent obviously and I have not said anything which I think will do any damage. There are cases at the moment, as I put it, in the pipeline about which there are concerns as to whether the police have had sufficient time to garner all the evidence that would have been available. There is an interesting article in *The Times* which I read on the tube this morning about this whole area. It makes the point that there is of course a lot of information available about the tools of terrorism, particularly very low-grade fraud. It is pretty easy to bring together the evidence of credit card fraud and other small frauds which are used to fund terrorism, but that is only at best, if I can use a football analogy, league one and it is neither championship nor premier league. If one is going to obtain the information that shows the premier league terrorism conspiracies, one needs to go far beyond that fairly basic evidence. It is like the whole question of drug crime where it is pretty easy to catch people who are small-scale street distributors, but it is much more difficult to catch the very big fish because it involves a great deal more work and that is more difficult in volumes, in multipliers in the world of terrorism, I believe.

Q100 Mr Streeter: Our friends from JUSTICE have made three specific suggestions which they prefer to the current detention provisions. The first one is developing the threshold test for prosecutors, secondly, bringing into force Part 3 of the Regulation of Investigatory Powers Act, and then, finally, allowing intercept evidence. Can you comment on how you react to that? Do you think they would be useful mechanisms or useful tools, particularly the use of intercept evidence which of course is a big political debating point?

14 February 2006 Lord Carlile of Berriew QC

Lord Carlile of Berriew: I agree completely with JUSTICE on all three points. I think they would all be helpful and useful developments. I think there is a danger of this whole intercept evidence issue, however, being exaggerated in its importance. My own view is that the use of intercept evidence in British courts would be very useful. I have been in the odd case in which intercept evidence was used, but it happened to be foreign intercept evidence, so it was admissible. For example, I was in a case where Dutch intercept evidence was used. However, I think that intercept evidence would be of greatest utility in catching people who have committed serious money laundering offences and drugs crime. There would be some cases, I suspect a very, very small number, in which intercept evidence could be useful in catching terrorists. I cannot see myself any good remaining reason why we should exclude its use. After all, it does not have to be used and it only has to be disclosed if its disclosure materially assists the defence case or materially undermines the prosecution case. That is the basic rule of disclosure, otherwise it does not have to be disclosed. At the end of the day, they do not have to prosecute either. I do think intercept evidence has a small potential for utility in this area.

Q101 Mr Streeter: But you do not think these three tools could replace detention?

Lord Carlile of Berriew: No, I do not think they would replace it. Of course when you say "detention", by that I understand you to be saying a reasonable period for investigation after arrest.

Q102 Mr Streeter: Yes, 28 days.

Lord Carlile of Berriew: No, I do not think they would replace it. They might accelerate the release time.

Q103 Mr Streeter: You have already commented on my next question, the police charging a suspect with a lesser crime and holding them in custody while gathering evidence for a greater crime, but could you just comment more fully on your views about that?

Lord Carlile of Berriew: This was the suggestion that I think was put forward most strongly by the Party to which I happen to belong early in the debates on the Bill. In France they arrest people for something called '*association malfaiteur*', and it does not come much vaguer than that, and incidentally the comparison of the French and Spanish system generally favours British human rights standards which I can go into in more detail if you would like. I do not believe that it is right for somebody to be arrested and charged with, and my analogy was shoplifting rather than murder, using telephone cards as currency, which is one of the things which has been done for asylum-seekers who may be interested in terrorism, when, in reality, what you are investigating is a big terrorism conspiracy. I think people should be charged, and prosecuted, for what they are thought to have done. I do not think it is fair to people to say,

"We're arresting you and charging you with a trivial charge", then put them in Belmarsh on a charge of credit card fraud, keep them there for the 18 months it takes to bring a really big terrorism offence to trial, much longer than 90 days, and then half-way through or near the end of that period say, "Whoops, terribly sorry, old chap, but we have not been able to get the evidence together, so if you kindly come down to the Woolwich Crown Court and plead guilty to obtaining telephone cards by deception, you will not get three months' imprisonment and you can go home". I think that is fundamentally dishonest and I do not agree with it. It is a very naïve view.

Q104 Mr Streeter: That is very clear. Finally, could I have your views on the use of tagging, surveillance, bail conditions or control orders as alternatives to custody in this area of course.

Lord Carlile of Berriew: I said in my recent report that I think more should be done to review the extent of the control orders as apply. That is really why I insisted on the standard control order being included in the report. I think the Home Secretary has accepted in principle now that there should be within the Department regular reviews of each case to see whether every restriction is really needed. My own view is that the control orders that are imposed at the moment, in all but one case, and that one case happens to be the only case where a British national is the subject of a control order, they come close-ish, some might say "perilously close", I would merely say "close-ish", to derogation. I think we are still on the side of non-derogation, but it could be challenged.

Q105 Mr Malik: I welcome Mr Winnick's intervention earlier on because I do think language is incredibly important. You talked about good imams and bad imams and obviously that describes them, but it does not give any sense of the quantum. The same equally is true for this notion of moderate Muslims and extremists. I think that actually undermines confidence, it deepens quite a mistrust, it reinforces all the stereotypes and it damages community cohesion. For me, terms like "mainstream Islam" would then give a sense of quantum and extremists obviously would be a small part bolted on to that somewhere. I just want to come back to a point, and that is why I am pleased that you asked about it, David, but I just want to come back to a point that you raised which was that, and hopefully it is a correction, that actually the last terrorist attack in this country was not in the name of a united Ireland, but it was in the name of killing black ethnic minorities, Muslims, Christians, whoever they might be, and it was David Copeland, the bomber in Brixton, Soho and Brick Lane where he killed three and maimed over 80. This is the real problem with this whole debate actually, that the focus in all the examples you gave, there was not any white supremacist, not any animals rights activist, there was not anything about Christian fundamentalists, anti-abortionists, and the focus was just Muslim, Muslim, Muslim.

14 February 2006 Lord Carlile of Berriew QC

Is it any wonder then that people out there think that this legislation is targeting Islam and Muslims when we ought to be saying that this legislation discriminates only on the grounds of those who would be engaged in, and involved with, terrorism and not on the basis of religion? The whole debate is extremely counterproductive, so how do we improve this debate?

Lord Carlile of Berriew: First of all, Mr Malik, I say, and I hope you will not think this patronising, that I have been hugely impressed by the way you have dealt with these issues publicly. I know the area you come from very well as I was brought up in Burnley and my mother still lives there, so I know the area extremely well, and I think the way—

Q106 Mr Malik: You are trying to endear yourself to me!

Lord Carlile of Berriew: We are both Clarets supporters, are we not! I think the way that what you have done has resonated has been very good. I would, however, throw the question back at you and say that I have merely responded to the questions that have been put to me and the language I have adopted in answers has been derived from the language of the questions. I agree with you entirely. I think it is very important that we should look at terrorism as a whole and it is very unfortunate that Muslims are feeling stereotyped by all this. It is extremely important that the police in particular, for example, when they are searching and stopping people at airports, should not stereotype. I have said that the number of section 44 searches under the Terrorism Act could be reduced by 50% without damage to national security and the number of Schedule 7 stops at ports could be reduced by the same proportion without risk to national security. Underlying your question is a dilemma though. I have been asked by the Government, and have accepted the task, to prepare a report on the definition of “terrorism” in British law, and this is going to take a number of months. I issued a call for papers recently and there are going to be public events if people wish to attend them and I hope they will. You raised a number of potential terrorism issues about which I have had questions raised with me about whether they are terrorism at all. Is, for example, animal rights activity a terrorist activity or is it just a very bad, common crime? There is, therefore, a genuine question about how wide the range of terrorism should be in law. The Bishop of Oxford, on the other hand, in a speech in the House of Lords very recently, and Bishop Harries is a man of great wisdom, proposed an extremely wide definition that would certainly have included the activities of the leader of the British National Party, a former constituent of mine, about whom I know much, too much, so I think there are difficult definition issues underlying what you say, but I will accept completely your thesis and I think we all have to learn how to deal with these issues, and some of them I gain from you actually as I listen to what you say.

Q107 Mr Spring: Just turning to your report and your recommendations based on the Newton Committee, you talk about the fact that the existing system of scrutiny is designed currently for short periods and you say, “a more searching system is required to reflect the seriousness of the State holding someone in high-security custody without charge for as long as three months”. Obviously we have, as you have heard, had representations and evidence from JUSTICE and Liberty. One of the things that arises out of their comments is that the current system of judicial oversight of pre-charge detention is invariably flawed because the adversarial system which operates in this country is one where the judge is likely to hear what the prosecution has to say and act accordingly. Now, in your proposals how do you feel that this contention of theirs and their concern could be dealt with?

Lord Carlile of Berriew: The concern is a legitimate one, but I think it is over-expressed. If you look at the performance, and I am only talking about the performance, of judges under the Diplock system in the courts in Northern Ireland, and I am not making a comment about the merits of the Diplock system, the judges who have been giving judgment for many years now in the Diplock courts in Northern Ireland have learnt a completely new discipline and they do it extremely well. They give reasoned judgments and actually the prospects of being acquitted in a Diplock court are higher than the prospects of being acquitted before a jury, as it so happens. Now, I thought very hard about the kind of judges who would need to do the work I suggested in my proposal and it seemed to me that we needed senior judges, and I mean senior in terms of competence as opposed to age though they may coincide occasionally, with great experience of criminal law, preferably people who have both prosecuted and defended in their practising years who, I believe, would happily adjust to a new system like this. The stereotyping of judges, of whom I know a large number, is almost as risky as the stereotyping of anyone else and I believe that, if one were to take the example of a group of senior judges at the Old Bailey, and there are others around the country, and asked them to do this kind of examining judge work that I have proposed, I think they would do it very well and adapt to it extremely quickly. Most of them have pretty rigorous minds and that is the most important quality needed.

Q108 Mr Spring: Thank you for that answer. Irrespective of the quality or qualities of the judges, specifically in your proposals you say that the judge should be provided with a “full and continuing account of all matters involved in the investigation in question”, but who do you think should prepare that sort of information for the particular judge in question?

Lord Carlile of Berriew: The Crown Prosecution Service basically, although I have suggested that there be added a special advocate there to scrutinise the material and make completely objective

14 February 2006 Lord Carlile of Berriew QC

representations to the judge, both orally and in writing, and of course to make contact with the defence lawyers. I would like to see the whole special advocate system operating a little more flexibly than it is right across the board.

Q109 Mr Spring: You talk about the special advocates and would such the special advocate who had received security clearance have contact with the detained person on whose behalf they were appearing even after they had been fully briefed on the investigation?

Lord Carlile of Berriew: I think that they certainly should have contact with the lawyers for the detained person whose interests they are representing, but on whose behalf they are not strictly appearing. I believe that it should be in the discretion of the oversight judge to decide the extent to which such contact should take place. There is a danger of compromise and of undermining the whole system and each case has to be considered on its merits, but I would hope that, compared with, say, the SIAC system, the special advocate would be able to come a little closer to the defence interests in the case.

Q110 Mr Spring: You talk about again the discretion of the judge and the sort of judge you have in mind and, as one of your proposals, you talk about the “suitable opportunity for written and oral defence representation against extended detention”. What do you envisage by a “suitable opportunity for written and oral defence representation against extended detention”?

Lord Carlile of Berriew: I do not think we should be too structural about this. The analogy I would take, I suppose, is the Woolf reforms, the civil procedure rules for civil courts where some work is done by the judge in chambers dealing in private, taking representations in writing, some is done on the telephone, which is a remarkable development for the legal system to have hearings by telephone, and some is done with hearings in a courtroom of one kind or another. I think the procedure should be flexible enough to enable the result to be right rather than there being a procedural straitjacket that might limit the prospects of the result. I think this is something that would have to develop. I see a group of judges doing this kind of job as something like a sort of collegiate body and with a great influence on their own rules and I would hope it would not be too formal.

Q111 Mr Spring: Lastly, and I think we can guess what the answer to this will be, but just for the record as it has been put to us, on the question of increased judicial oversight, there is some criticism of your suggestion on the grounds that there are incompatible elements here of an examining magistrature and the common law system. Do you see any incompatibility in those?

Lord Carlile of Berriew: I did, but I have been persuaded, partly by Newton and partly by looking year after year at these issues, that the common law system, which after all is built on flexibility, a

system of precedent built on the potential for change, is more capable of adapting itself to this kind of requirement than possibly the continental systems are. I had a meeting very recently with Juge de Brugiere, the very celebrated and very able French number one *juge d'instruction* in these terrorism matters, and I asked him a number of questions and was slightly appalled by some of the answers. They do not tape-record interviews and, during the first two days of arrest while the suspect is under arrest for *association malfaiteur*, he does not have a lawyer present. He said to me, “Monsieur, this is a very productive period of interrogation”! I am not surprised because I practised at the Bar before the Police and Criminal Evidence Act 1984 when tape-recordings came into force. Now, I think our system is more flexible than that. I pointed out to him that in my local Welshpool Police Station they have a tape-recording suite, and it is not really very difficult to provide it. I think our common law system is adaptable. If you talk to French or Spanish lawyers, they say to you, “Well, I wish we had some of the elements of your system”.

Q112 Mr Clappison: I was very struck by the point you made that a number of cases which would need the longer period of detention is very small, but of course there is a strong public interest in making sure that every such case, and there will be serious cases, is properly investigated and, where appropriate, brought to justice. You have also been asked about the case which you told us of where significant conspiracies have gone unprosecuted and you told us a bit about that, but I wonder if you can just take us through the mechanics of how it is that those cases come to go unprosecuted because for somebody who is in detention at the time and they are released, they can still be charged later on, can they, with sufficient evidence?

Lord Carlile of Berriew: Let me give you a hypothetical answer, but it is not beyond the bounds of reality. Supposing the police arrest a young male who shows physically all the signs of being a suicide-bomber. He has prepared himself physically, and there are certain physical signs which are well known, and he has prepared his life, as it were, to become a suicide-bomber. The police arrest him and they have more than reasonable grounds for suspecting that he is a suicide-bomber, perhaps they have had a tip-off, but they know nothing or next to nothing about his connections. Now, they have taken him out of circulation by arresting him, and that is fine, he is not going to be a suicide-bomber, but, if he is a suicide-bomber, you can rest assured that he is unlikely to be the only one in a group and there is likely to be some kind of cell and they need to discover more. If that person sits in Paddington Green or Govan or the custody unit in Northern Ireland, which I visited very recently, and says, “I’m terribly sorry, but I’ve been advised to say absolutely nothing”, which is going to happen in possibly 100% of cases, then it is actually very, very difficult, as it is a very slow process, to put together his life and times, his

14 February 2006 Lord Carlile of Berriew QC

connections, years of associations, his travel details over the last five or six years; it is a slow process. I think that is quite a good and realistic hypothetical example of how one individual could lead to great investigative difficulties. Of course there is a particular problem if, say, eight individuals are arrested. You may have the same lawyers representing all or some of them. The Paddington Green process, the police will tell you rightly, is an extremely slow process because they do properly respect various aspects of the personal lives of the people concerned and certainly 14 days can disappear very quickly and there is an awful lot of administration. I hope that answers your question.

Q113 Mr Clappison: I find that very helpful. Bringing to bear all your professional experience and also the experience you have had of four years in this post, you are telling the Committee then that, without the longer period of detention and taking into account the possible alternative courses of investigation, there remains a risk that a significant conspiracy would go unprosecuted?

Lord Carlile of Berriew: Yes.

Q114 Mr Clappison: Can I now ask you about a completely different subject. You were talking earlier on about the period in life when young people are very impressionable and you mentioned the influence that some extremist preachers would possibly have. You also mentioned universities and, for the sake of completeness, people could be influenced by extremists of many different kinds at university.

Lord Carlile of Berriew: Of course.

Q115 Mr Clappison: Just taking this area, can you say a bit more about the concerns which you have got in that area because what happens in universities is a matter of great concern?

Lord Carlile of Berriew: This is entirely anecdotal, so I really would not pretend that I have evidence that I, as a lawyer, would regard as evidence, but, talking to young people, I believe that what I said earlier is true, that there are some societies in some universities which are very exclusive. They may include the sort of societies Mr Malik was talking about outside of anything connected with Islam at all, and I am sure there are many of them. Some of those might be all-female societies, there is exclusivism everywhere, but I am led to believe that there are some pretty intimidating groups in some, I suspect a small number of, universities. Nobody wants to inhibit people who are going through that very important education process that the university degree provides from being as conceptual as they like, their imaginations running riot, but there are dangers too.

Q116 Mr Clappison: Do you know anything about the attitude of university authorities towards this?

Lord Carlile of Berriew: No.

Q117 Chairman: Lord Carlile, you have been enormously helpful this morning, drawing on your deep experience. Can I put one question to you and it is really asking, if I may, for your advice to myself, as Chairman of the Committee, as a whole. Much of the powerful evidence you have given depends on the information which is necessarily confidential and indeed last week witnesses said to us, "Well, you should just dismiss Lord Carlile's views because they are not based on public information and we cannot rely on them". As a committee, up until now we have chosen not to meet in private session, where we could of course get some of this information in a confidential session, largely, I think, because we are trying to judge these matters as other members of the public have to judge these matters on the basis of the publicly available information. If we get confidential information, we are putting ourselves in the same position as you and we cannot explain why we have reached any conclusions we have. Do you think it is absolutely intrinsically possible to reach a balanced judgment about the correct period of pre-charge detention without having access to information which is necessarily confidential because it is about past or current police inquiries?

Lord Carlile of Berriew: No, I do not. I think, if I can answer the question in a slightly different way because this concerns me every day of my life, there is a trust issue, there has got to be a trust issue because not all information can be given publicly. The trust issue has been very damaged by intelligence information connected with the Iraq War which is perceived, rightly or wrongly, and I make no judgment on it, to be inaccurate, particularly what is described by the press as the "dodgy dossier". That has had a devastating effect on the level of trust given to MI5 or to anyone like myself. I do not see that much and the press exaggerate what I see, who is able to what I ask to see and I am not refused anything that I ask to see. We would like to be trusted and we would like the public to believe what we say. The effect of past events means that we are not trusted as we would like to be. It is a matter for a committee like this whether you take it on trust or whether you get to see more information, and of course it is a matter for government as well in the end what they show you, but I do not believe one can make a fully objective judgment without seeing the information, unless you are prepared to say, "Well, we'll take certain things on trust". Eliza Manningham-Buller will tell you in general terms roughly what I have told you, I think, and I see no reason not to trust her, far from it, but it may be of reassurance to the public if you were to see more. It is a matter for you, sir.

Chairman: Well, that is very helpful and something the Committee will need to reflect on during the rest of the programme of this inquiry. Lord Carlile, you have been enormously helpful and thank you very much indeed.

Witnesses: **Professor Ross Anderson**, Foundation for Information Policy Research, **Mr David Lattimore**, Technical Manager, Digital Crime Unit, LGC Ltd, and **Mr Peter Sommer**, London School of Economics, gave evidence.

Q118 Chairman: We are moving on now to some of the more technical issues. We are very grateful to you for joining us today. I wonder if you could introduce yourselves for the record.

Professor Anderson: I am a Professor of Security Engineering at Cambridge University and I also chair the Foundation for Information Policy Research.

Mr Lattimore: I am David Lattimore. I am the Technical Manager of the Digital Crime Unit at LGC Ltd. I have been involved in computer forensics since 1992 and I still carry a caseload today, so I have quite a bit of experience in that field.

Mr Sommer: I am Peter Sommer from the London School of Economics. I am an external examiner at the Centre for Forensic Computing at the Royal Military College of Science, which is where a lot of law enforcement agencies get their training, and I am also the joint lead assessor in this particular area for the Council for the Registration of Forensic Practitioners, which is a Home Office initiative to improve the quality of forensic work on the ground.

Chairman: Thank you all very much for joining us this morning. Part of the case for extended pre-charge detention is the difficulty of obtaining computer-based information and so on, so I hope this morning's session should shed some light on the truths and otherwise of that.

Q119 Steve McCabe: Does it surprise you that the three of you have such different views about how easy it is to access information on a computer? I wonder if I could ask each of you in turn to tell the Committee how you think it is possible in practice to access data and analyse it and how long you would normally expect this to take. If possible, could you account for the fact that there are such variations in the written evidence that you have provided to the Committee?

Mr Sommer: I have not seen Mr Lattimore's evidence. To a certain extent you are in length of a ball of string territory. The purpose of the sort of evidence that I have been trying to provide is to arm you with the variables so that when you come to seeing the police and others you have sensible questions to put to them, you do not have to accept it at face value. In broad terms if you are examining a computer you do not need initially to make a copy of it. In his theoretical case study which he provides you with Mr Hayman says that it takes 12 hours. In fact, all of the leading products allow you to carry out what is called a preview, which is where you can be examining a computer safely so that you are not altering any of its data, within a few minutes of getting hold of it. What I believe you are concerned with in terms of your particular inquiry is not getting absolutely every bit of evidence that you are going to be producing in court but getting sufficient in order to be able to charge and, depending on how you manage the situation, you should be able to do that relatively quickly. That prompts me to make a mild criticism, if I may, of Mr Hayman's statement. I am sure it was done entirely sincerely. It seemed to me

that he did not have a full grasp of how computer forensics works in the detail. Courses are available for line managers not to do the detail but to understand enough to be able to manage the situation properly. I greatly admire what he does, but I wonder if he would benefit from going on one of those courses. If he did so, he might be able to shorten considerably the period he seems to be going through. I am also relying partly on my knowledge of some of the cases that he is holding because I am instructed by the other side for them.

Q120 Steve McCabe: In your evidence you say it takes 30 minutes to image and one of the other witnesses says it is a process that often happens overnight. That sounds to me like quite a variation and I am not an expert like Mr Hayman.

Mr Sommer: Let me tell you what is involved. With the regular products you can look at about two gigabytes a minute and with a standard computer you pick up from the high street at the moment you are talking about 80 gigabytes hard disc, so it will take you 40 minutes to do the imaging. There is an exception and that is if it is a lap-top computer where you cannot pull the hard disc out it will take a great deal longer. I know Mr Lattimore reasonably well. We have not discussed our respective submissions. Maybe we will have a disagreeable appearance of argument in front of you.

Q121 Steve McCabe: But 30 minutes would be your expert advice to the Committee, would it?

Mr Sommer: I think you can get going on a preliminary exercise in 30 minutes but not an exhaustive exercise. It seems to me it is the preliminary exercise you are concerned with in terms of your inquiry. It is not getting final evidence you are concerned with but rather that it is enough to get to a charge.

Mr Lattimore: With imaging computers it varies greatly from the type of hard disc, the amount of data on the disc, the software you are using to image with and the hardware you are using to image with. There are lots of factors involved. I have a technician whose sole job is to image computers daily and we have computers in every day of the week and most of the computers he images do take overnight imaging. They may finish at four o'clock in the morning or three o'clock or eleven o'clock, but we do leave them overnight to image. We have always used previewing as a form of investigation, but invariably what we find at the end of the day is we then go on to image that computer. An initial investigation is only to say whether we have got something there or not. Invariably all our computers are imaged because at a later date somebody will want a copy of that image.

Professor Anderson: The point that I was making in my submission is that the amount of data that the police sees, and also in civil matters, is going up very, very rapidly and the police are falling further and further behind. A PC may have 80 gigabytes at the moment whereas a few years ago it would have been a few gigabytes and I would think that in 10 years'

time when the police raid someone's home they might find dozens or perhaps hundreds of computing gadgets on which data can be stored. It is common nowadays, for example, for people to back up their data on devices like an iPod and so in future when you raid somebody's house you will seize their iPod and see if there are data files on it. This business is going to be more complex and the police require a step change in their capabilities in this regard.

Mr Lattimore: In one case last week we had a person who had five computers submitted from his home address and nine hard drives and all these hard drives had been to his work address and used in the machine there as well. To do that amount of data is very, very time consuming.

Q122 Steve McCabe: With the exception of Mr Sommer, the other two witnesses are suggesting that the police case for 12 hours is not that ridiculous. Mr Sommer said that Mr Hayman did not understand it and he should go on one of these courses. In the police evidence they talk about a minimum of 12 hours to try and access this data.

Mr Lattimore: If you asked me to do an investigation and give an opinion in 12 hours, I would be happy with the evidence I had given.

Mr Sommer: It is purely imaging he is talking about, not the investigation.

Mr Lattimore: It all depends on the hardware you are dealing with and the software and what is on the hard drive because it can vary. A 200 gigabyte hard drive may only take 20 minutes if there is very little data on it, but if there is a lot of data on it it might take overnight.

Q123 Steve McCabe: Do you know what role the information obtained from computers plays in charging suspects as opposed to simply building the case?

Mr Sommer: It depends entirely on the circumstances. It will vary considerably. Sometimes the computers are at the heart of it and sometimes they are entirely peripheral. That applies to any form of crime in which computers are involved as well as the terrorist cases. I currently am instructed in three terrorist cases and in one of them the computer evidence is really fairly peripheral, but there are a lot of other types of evidence in terms of what was located. The computer evidence may slightly strengthen or slightly weaken the police case but in other instances it can be absolutely at the heart of it, particularly if you are charging people with a conspiracy where you have to infer a common purpose and you will tend not to write convenient letters to each other saying "Let us conspire to X, Y and Z". You then have to say there is a pattern of behaviour or a pattern of surveillance of targets or whatever it is which tells us that something might be going on and people are working together. So there is absolutely no straightforward answer to your question. I understand why you are putting it but there is no easy answer.

Professor Anderson: In conspiracy cases critical evidence may come from traffic data obtained from phone companies. There are some particular types

of offences where material from the machine in question is critical to charging decisions, child pornography being an obvious case.

Mr Lattimore: I would tend to agree with both Peter and Professor Anderson. Out of all the computers I investigate, 70 or 80% of them are relevant to the charge.

Q124 Chairman: When you say relevant to the charge, do you mean needed before the charge is made?

Mr Lattimore: Yes, the data on the computer is relevant to the investigation. I deal with a lot of fraud cases along with various law enforcement agencies and they come to me with their computers and that data is used to prepare those charges. The one thing the police miss is the intelligence that is available on these computers. I know from all my years of investigating computers that nobody has taken this on board because the computer is a wealth of intelligence that is missed all the time these days. They have not got the time to deal with it, that is the problem.

Q125 Steve McCabe: I do not think anyone doubts its value, I think we were simply trying to establish whether it was central to the charge and it sounds like the answer is it could be but it might not be. If decryption and analysis was the subject where the greatest weight was placed in determining a period of detention pre-charge, how long do you think that detention period would need to be?

Professor Anderson: In the case of decryption, there are still a few products around where the act of searching for a key may take time, but this is largely a thing of the past. Encryption products nowadays tend to be either good or useless, and if they are good then you either guess the password or you give up. In the future world, for which I hope we are legislating rather than the world that is in the past, I think you can reckon that the majority of the effort will be put into the analysis stage rather than into technical aspects such as seizing the evidence, bagging it, imaging it, decrypting it and so on and so forth, but the human effort will be the limiting factor. Hopefully if the tools become better that will be the main thing that you will have to worry about, ie how long an analyst can usefully work on the data before he either stops finding stuff or simply becomes weary and gives up.

Mr Sommer: I have been following this as a parliamentary issue for rather a long time. When the legislation that is now in Part 3 of the Regulation of Investigatory Powers Act began its life in Parliament it was part of the Electronic Commerce legislation and I was the Trade and Industry Select Committee's specialist adviser then and I did a great deal of thinking about how it was supposed to work. At the time one of the things that the members asked the then Director of the National Criminal Intelligence Service was how big a problem it was and whether he had any statistics and when he was pressed he said they did not have statistics but that it was going to be a huge problem. They then asked for more detail and they came up with one case. I had

14 February 2006 Professor Ross Anderson, Mr David Lattimore and Mr Peter Sommer

predicted along with everybody else that encryption was going to become a much bigger problem than in fact it appears to have done. Let me give you an interesting analogy. If you look at Internet paedophilia, National Crime Squad Operation Cathedral looked into the group called the Wonderland Club and the very sophisticated people using encryption. I worked on the case professionally. Some of the encryption could not be broken. At the end of that all of us involved in that said it was a big, big problem. Fast forward to the famous Operation Ore which started up with 7,200 suspects who had subscribed to paedophile sites and whose database was held in a computer held in Texas. Out of those 7,200 suspects—and I purposely got an informal figure from the National Crime Squad last week—there have only been 20 instances where encryption has been a serious problem. It may well be that although it is there as a problem, operationally it is a little less big than it was. I hope you will ask the Home Office and the National Technical Assistance Centre, the people who do the job, for their statistics. In my written submission I describe certain types of encryption and I hope you will get some statistics from them in the way the Trade and Industry Select Committee failed to do a few years ago.

Chairman: We will follow that up.

Q126 Mr Clappison: Could you tell us how easy it is in your experience to identify the presence of encrypted material and how effective the police's forensic tools are for dealing with it?

Mr Sommer: The first thing you do when you start examining a computer is to say what programmes are installed and where is all the data held. If someone has got encrypted material on their machine the first thing you are going to be seeing is an encryption or decryption programme which as an experienced person you will know about. Often those programmes are not deployed but they are there if you start looking for them. What you find with a lot of the encryption programmes is that the first few characters in the encrypted file are always the same and you can search for those signatures. By doing a rough exercise and saying "Is there encrypted material on this computer?" though you may not be able to decrypt it you do get a fairly quick sense. Looking at steganography, which is the technique of hiding information inside pictures, which in my experience is more talked about than actually seen, again there are some very interesting steganography detection programmes. You can detect it fairly quickly. You know whether it is going to be there. That may then, if you were going to introduce properly Part 3 of RIPA, give you a basis for asking for the key or punishing somebody who is willfully declining to give you the key.

Q127 Mr Clappison: You have just told us that encrypted material is not as widespread as people once feared that it might be, but the sophisticated encryption which you have just told us about, how frequent a problem is that in your experience?

Mr Sommer: It seemed to be rather less than people imagined. I work mostly for the defence, but I talk to a lot of prosecutors and the police and various other services because there is a fairly free interchange at a certain sort of level. My impression is that it is not as big as most of us thought it was going to be, but you must ask the Home Office witnesses yourself as they will have a much better overview.

Q128 Nick Harvey: How frequent is it to find the key to sophisticated encryption through the carelessness of the user?

Mr Sommer: You point your finger at one of the main techniques that is used. With people using sophisticated techniques you probably are not going to be able to break the system. You can forensically examine a computer and you may find the key or you may find part of the stuff is encrypted in plain text form. It is one of the most important techniques that you use.

Q129 Nick Harvey: Would bringing in Part 3 of RIPA help?

Mr Sommer: I think it would. Obviously there are broader issues which I am not here to discuss that are human rights aspects to do with people not being forced to self-incriminate. At a practical level, bearing in mind the way Part 3 is supposed to work, if it does go before a jury and if you say you have lost your key the jury have to decide whether you really have lost the key. It would be an important tool if only because you would be able to disrupt a suspect. I think you need to explore why Part 3 has not been brought in and that was basically because the Home Office was overambitious in producing its detailed proposals. There is very little difficulty in terms of legislating for stored data, in other words data found on a hard disc. They also wanted to introduce it for data in transmission, but you then run into problems with the techniques used by the financial services industry when they use what are called session keys, ie every time you transact the key changes and nobody knows what the key is at any one time, so forcing disclosure becomes difficult. What should have been done and maybe still should be done is to try and do the easy stuff because it is going to be helpful and we will leave it to some sort of think-tank people to come up with a solution to the more complicated stuff.

Mr Lattimore: The problem with Part 3 is that if I was a suspect and I had encrypted data on my computer I would quite happily go to court and take the two years because I know I am going to be out in a year's time. A terrorist or a paedophile is going to take the two years, that is the big problem.

Mr Sommer: You are still disrupting the terrorist's units, which is an important element of what Alex Carlile said to you earlier on.

Professor Anderson: I tend to be slightly sceptical about this. Okay, it may provide holding charges to get people that you cannot get on any other basis but, given the extremely low prevalence of encryption use by bad guys, quite frankly you would be better getting after them for tax evasion or social

security fraud. I am not sure that it is a good use of the senior management time in the Home Office pursuing such a small and specialist matter.

Q130 Nick Harvey: Have you any other suggestion for plugging gaps in this area of legislation?

Mr Sommer: Remove the bar on the interception of telephone evidence.

Q131 Chairman: No, in terms of computer data.

Mr Sommer: Trying to interpret Parts 1 and 2 of RIPA, whether it is content or communications data, is becoming increasingly difficult because of the problem of legal interpretation. The legislation has been drafted in terms of making a distinction between the voice component and the traffic component—who contacts whom, when and for how long—and it makes it much more difficult when you are dealing with e-mails or web-based e-mails or voiceover Internet protocol or things like that. There are going to be problems which are completely unavoidable.

Q132 Nick Harvey: Could this be updated with the right technical advice?

Mr Sommer: Updated in what terms?

Q133 Nick Harvey: To try and address these moving targets that you are describing.

Mr Sommer: I think it is going to be impossible. If you look at the behind the scenes discussions about interpretation in terms of Part 1 and Part 2, the affected Internet Service Providers and if you look at what you type into a web browser when it is content and when it is traffic data, there are suggestions and understandings but they have not been tested in court yet.

Q134 Nick Harvey: How helpful are manufacturers of encryption software? Can they provide a key to anything that is generated using their products or is it possible for someone else to develop encryption and maybe sell it on in a way that the manufacturer cannot determine?

Professor Anderson: I think what you have to watch out for here is that from later this year the encryption landscape is going to change with the release of Microsoft Vista, the next generation of Windows operating system, which will support the use of a chip called a TPM which manufacturers are putting on PC motherboards. What this means is that by default your hard disc will be encrypted using a key that you cannot physically get at. This is being done for a number of commercial reasons: firstly, to do digital rights management on downloaded music and films and, secondly, by the software vendors so that they can lock the customers in tightly and charge more for their products. An unfortunate side effect of this from the point of view of law enforcement is that it is going to be technically fairly seriously difficult to dig encrypted material out of systems if people have set it up competently. One issue that was in fact discussed at APIG here a couple of weeks ago is whether there might in the medium term be some kind of obligation placed on

computer vendors, hardware vendors like Intel or software vendors like Microsoft, to see to it that 'back door' keys be made available. Certainly if I were running the appropriate department in the Home Office I would be getting into conversations with Microsoft about this issue now rather than in November when the product is shipped.

Q135 Mrs Dean: How widespread are the skills needed to decrypt computers? How much training is necessary to bring someone up to the required standard? Can one expert supervise a team of less skilled analysts?

Professor Anderson: Once we achieve maturity in this field you will see a hierarchy of skills in the police and elsewhere. At present and over the last 20 or 30 years the police have tended to see computer experts as being a breed apart. You had a detective constable here and a detective superintendent there whose hobby happened to be computers rather than yachting and so he got called in when there was some complex business going on. That is not going to wash in the modern world because computers are everywhere, in our lives, in our homes, in our businesses. In future, rather than thinking of the computer expert as the guy in a white coat with a degree and a Home Office licence and all the rest of it, you are going to have to see basic computer skills embedded at all levels in the police force and elsewhere, amongst civil litigators for example, because this issue affects civil as well as criminal matters, and then there will be a hierarchy of people with perhaps slightly more expertise, people who do regular retraining of detective constables and then higher up there will be the PhD grade people who are involved in designing the next generation of tools. At present we do not have anything like that ecology of forensic expertise.

Mr Sommer: I agree broadly with Ross's analogy. I think the situation may be slightly better than he is describing. If we look at the people at the National Technical Assistance Centre, I know a number of them, they do not talk a great deal about their work, but I have known them in previous jobs and I have also seen their academic work and articles they have written. These are broadly speaking people who are highly adept at using tools that have been created by others. If you go back to Ross's reference to a hierarchy, there are people who have come out of law enforcement and who do this sort of work and operate at the second layer; in other words they use tools created by others very, very intelligently and that is probably the greatest need. At the top level, when you have got something that is really new and really difficult, Doctoral level as opposed to Masters level, then I suspect they have to go to Cheltenham or there are a few private sector places where they can get it. NTAC, even if you know the people socially, is not an organisation that chats a great deal about itself, but I do hope from your position as a parliamentary select committee you can ask them about these issues based on the background that we are able to give you here today.

14 February 2006 Professor Ross Anderson, Mr David Lattimore and Mr Peter Sommer

Mr Lattimore: I was involved in NTAC. I am not going to go into too much detail about it. I set it up with a number of other people and I was operational in there for a number of years and our success rate was very, very good, but it is not just a matter of brute forcing encryption, there is a lot of work that goes in by a team of people that all work together, all with different skills and that is the way forward for dealing with encryption in the future.

Q136 Mrs Dean: If the police had twice as many computers and skilled operators, would it mean that they could achieve the results twice as quickly as they do now?

Mr Lattimore: No. The police would never ever be able to deal with this type of encryption because (a) they have not got the time and (b) they have not got the hardware to deal with it because you do need specialist hardware which most police forces cannot afford to purchase and that is the beauty of NTAC.

Q137 Mrs Dean: So what you are saying is that there are the resources available but the police have not called on them, are you not?

Mr Lattimore: Some police forces call upon them and some do not. Some see it as they have failed in what they are doing. Some used to use us all the time and our success rate was in the 70% range which was very, very good.

Q138 Mrs Dean: Do the police need to reassess their approach to decrypting computers, and is the volume of evidence available, or potentially available, on computers effectively unmanageable?

Mr Sommer: I think that sort of exaggerates the position. What we are trying to do is avoid making these sweeping statements. There are situations when life is jolly difficult, but then that is no different from any other sort of crime when a police officer may feel there is a bit of evidence if only he could find it. The fact that they can see it there is a small part.

Q139 Chairman: I want to pursue this point because this is at the heart of our inquiry. You have been very helpful in explaining more about the processes and the issues. I think all three of you in different ways have made it clear that the technical issue of decryption itself does not justify the 90-day detention period because it is the analysis of what you get from the computer that is most important to the possibility of laying charges. Could each of you just briefly say from your knowledge of this field whether you think the difficulties in the process of decrypting and analysing information provides support to the idea of an extended period of pre-charged detention in terrorist cases and, if so, how long? That is the crux of the issue. You have set out the issues and how it works very clearly for us. Does this justify the case for an extended period of pre-charged detention? Professor Anderson, you were very clear in your evidence that encryption per se did not justify the 90-day detention period. If you take the process of encryption and analysis, in your view does it justify extending the period of pre-charge detention and, if so, how long?

Professor Anderson: I do not think it makes a very strong case. I do not have huge experience of terrorist cases; I have only been instructed in one of them. I have done a number of other crime cases and a large number of complex civil cases. In my experience people take as much time as they have got. Even if you have got a civil case that drags on for months and months and months, the work is always done in a rush just before the deadline to submit papers. I think that if a case is to be made for extended time limits then perhaps what the Committee should consider is whether there is any noticeable difference in outcomes between Scotland, which has got very, very tight time limits at all parts of the judicial process, England and countries like, let us say, France and Spain which can be very much more dilatory. My view tends to be, based on my experience of these things, that you work for a certain amount of time on a heap of data and then you run out of ideas or you run out of puff or you run out of money. Whether your two weeks of intensive work forms part of the 110 days that you have in Scotland or part of the two years that you have in England or part of the five years that you have in Italy probably does not make much difference to the amount of work that is involved.

Q140 Mr Winnick: I will take that as a no!

Mr Lattimore: I believe you have got to judge each case on its merits. Every case has to be looked at to see how much data you have got and whether you need the 90 days. Lord Carlile said about having a judge there to look at the evidence. The judge needs a team behind him, IT specialists who know this field and who can advise him on the data that the investigators are looking at.

Q141 Chairman: Taking Professor Anderson's point, can you think from your own personal experience of a case where somebody or a team has worked flat out for 90 days?

Mr Lattimore: Yes, myself. I have worked on cases that have taken longer than 90 days to crack. I am not going to go into the techniques I use because I want to keep them out of the public domain. You do a lot of work in the background before you mount the attack on the encrypted data and once that work has been done you have got somebody else that may have to write a programme to attack the data, then you put it onto a very big computer and the work goes on. If it is not done after 28 days you are not going to get it done at all. It normally comes about very quickly once you have done the initial work. That work used to take me three or four weeks. I would be sat at my hard drive doing a lot of biographical programming on a suspect for three or four weeks. It is very time-consuming work.

Mr Sommer: I agree with what everyone has been saying.

Q142 Chairman: Professor Anderson and Mr Lattimore have said two different things.

Mr Sommer: In terms of their experience, I could pick up bits from both of them. I do not think that you can look at the encryption issue and say this is

14 February 2006 Professor Ross Anderson, Mr David Lattimore and Mr Peter Sommer

what is going to tell us what the period of time ought to be; it does not really help you. If you are looking, as you are, at the other arguments against having extended periods then, on the encryption issue, there is nothing magic that we can tell you and say “Oh, yes, there is a magic figure to do with the period involved in decrypting which will now help us fix the time”.

Q143 Chairman: On the process of decryption and the analysis of what you then get, if you take those as the two key elements put together, do you see from your experience of these cases a justification for saying the police may need up to 90 days to carry out those processes before making a charge on occasions?

Mr Sommer: In that case I will side with Lord Carlile. In other words in a very small number of instances there may be a case for it. It is only supportable in the terms on which he was putting it to you, which is a highly detailed review. I think Dave Lattimore’s suggestion to you that this team that Lord Carlile is talking about would almost certainly need to be augmented by IT advisers specific to whatever special advocate or supervising judge he might have—

Q144 Mr Malik: So on rare occasions up to 90 days could be justified?

Mr Sommer: On very, very rare occasions, yes.

Chairman: Thank you very much indeed. It is a very complex area. You have covered it very clearly in a short time.

Witnesses: **Mr Daren Greener**, Systems Technology Consultants Ltd, **Mr Vinesh Parmar**, Telecoms Forensic Technical Manager, Digital Crime Unit, LGC Ltd, and **Mr Gregory Smith**, Principal, Trew & Co, gave evidence.

Q145 Chairman: Good morning. Thank you very much for joining us. As you know, we are carrying out an inquiry into the case for extended pre-charged detention. In the latter part of today’s sessions we have looked at some of the technical arguments that the police have put forward for extending detention while they gain evidence that might be used in a charge. This session is going to look particularly at mobile phone technology in the broadest sense. I wonder if you could introduce yourselves very briefly for the record and then we will begin the questioning.

Mr Smith: My name is Gregory Nigel Smith. I am Principal in the firm of Trew & Co. I have been involved with mobile telephone evidence for over 17 years, 13 years of which have been dealing with the current technology called GSM and three years with the new 3G technology. I run training courses for law enforcement agencies to educate them in this area of mobile telephone evidence. I conduct expert evidence in relation to mobile telephones and some other devices. I work for both the prosecution and the defence.

Mr Parmar: I am Vinesh Parmar. I have been working with the forensic mobile team for approximately five years now, primarily with Thames Valley Police as a forensic analyst. I am now with a company called LGC doing the same type of role.

Mr Greener: I am Daren Greener. I work for a company called Systems Technology Consultants. I have worked as an expert witness investigator on mobile phone evidence for the last four years. I present evidence on a range of issues, from mobile phone examinations, billing analysis and sub-site analysis predominantly in criminal cases in the UK.

Q146 Mrs Cryer: I would like to ask you some questions about obtaining data from mobile phones. I wonder if you could describe for us the role played in charging suspects by information obtained from

mobile phones rather than in building the final case. Do you expect this to change in the future? Would you like to see change in the future?

Mr Parmar: It is definitely going to be case dependent or inquiry dependent as to what value the evidence would have, if any at all. There have been cases where it is the only evidence in terms of being able to charge a particular suspect and in other cases it has been a question of showing a particular pattern which leads on to the charging of a suspect.

Mr Greener: I would agree that it is very much a crime dependent thing. A lot depends on the crime itself in relation, for example, to threatening behaviour and things like that. It may be the messaging and the content of text messages which are on there that is important. We may have videos and image sources that may relate directly to a crime that has been perpetrated.

Q147 Mrs Cryer: Could you describe for us the causes of delay in obtaining and analysing information from mobile phones? Should it be determined that this be the main factor in determining the length of pre-charge detention? Could you suggest how long this pre-charging detention should be to accommodate this sort of inquiry?

Mr Greener: Delays can be included from the start. The actual phone may not come to the analyst straightaway as it may be subject to DNA evidence or another type of evidence for drugs and things like that. When we finally get access to the phone there may be problems with the phone itself, ie it may be PIN locked. These obstacles need to be overcome. When we come to looking at the data and the phone, sometimes it is the case that the phone needs repairing or there is no charge in the phone. There is a wide variety of handsets available on the market today and we have to find the right charging equipment and things like that which is not always available. There are initial delays before we start analysing the data and then we come on to other

14 February 2006 Mr Daren Greener, Mr Vinesh Parmar and Mr Gregory Smith

issues that may be to do with the sheer volume of data on these phones nowadays that have very high capacity levels.

Q148 Mrs Cryer: So there is a variety of reasons for the delays.

Mr Greener: Yes.

Q149 Mrs Cryer: And therefore you cannot suggest a period that would be needed to produce evidence prior to charging?

Mr Greener: No. It is always done on a case-by-case basis.

Q150 Chairman: Are we talking hours, days, weeks, months?

Mr Smith: One cannot use one particular technical problem to hijack everything as I do not think that is correct. If you obtain a mobile telephone that has no PIN or PUK connected to it, there is no reason why you cannot turn the evidence round within seven days. People are concerned that if they have a mobile telephone that has been password protected three or four times and that causes delays then everyone should quote the worst case scenario but that is not the case. We are not dealing with the worst case scenario. If somebody picked up 20 or 30 mobile phones you may find one or two are problematical but the others would not be a problem at all.

Q151 Mrs Cryer: So far as your experience is concerned, how useful is information obtained from a mobile phone handset without accessing the supporting data from the network providers? How long do you believe they take to provide the necessary information?

Mr Smith: There are two sides. Whether the data on the handset has any substantive evidence in court largely depends upon how it relates to the crime. Quite often I have seen a judge saying, "I see an SMS text message here on the handset. Have you any substantive proof by way of a calling that it was sent?" and when we say we have not they kick it out and say they do not want it. The other side of the coin is that a lot of the work that they do with mobile telephones very rarely comes through into evidence, it is used for intelligence, which is a completely different matter and has got nothing to do with the detention of people.

Mr Parmar: I would agree with those points. The actual data that is produced in a report format is pretty meaningless unless there is network data to corroborate subscriber checks and billing records and so forth. Without that the actual data is going to be meaningless.

Mr Greener: One of the factors about a lot of the data contained within the phones is it is time stamped by an internal clock on the phone that is programmed by the end user of the phone and that is why we need to obtain the billing data, to confirm whether these events recorded within the phone are correct or not.

Q152 Mrs Cryer: From the providers?

Mr Greener: Yes.

Q153 Chairman: How long does it normally take for network providers to provide the necessary information?

Mr Parmar: It depends on the level of the crime. They have got to have five levels and they are graded one to five.

Q154 Chairman: What about if it was a terrorist case?

Mr Parmar: Level one is a threat to immediate life. So it really depends on whether the particular terrorist incident dictates that. If it is a level one incident then it is usually within two to three hours or, for the worst case scenario, it would be within 24 hours that the information would be available. That is not just obtaining data from the UK networks, that is also obtaining data from non-UK networks.

Mr Smith: It is severity that produces those speeds.

Chairman: Obviously we are asking you general technical questions but we are centred on terrorist investigations. I think it is reasonable to assume it is towards the upper end of that.

Q155 Mr Malik: Are you detecting an increase in the encryption of data on mobile phones? Is that a trend that you are starting to see or not really?

Mr Smith: No, I am not seeing any increase at all. It is probably not happening at all.

Mr Parmar: I have had a few instances over the last few months where I have experienced encryption to do with external components associated with the handset in terms of memory cards. At the moment there is no solution.

Q156 Mr Malik: Can you expand on the memory cards point?

Mr Parmar: What we are seeing now is a change in technology, a trend towards additional storage capacities within the handset itself. What most manufacturers are doing is not only giving you an internal memory store but giving you an expandable memory store by way of a memory card, which is basically just a small chip which can vary in terms of capacity so far as memory is concerned. It is mainly used to store multi-media files in terms of pictures and videos, but I have seen cases where other data can be stored on there which is not detectable by the device itself. There is an element on some of these devices whereby you can password protect it. It is not a very strong encryption but nevertheless there are no tools that allow us to start decrypting that information, but not enough is known about it at this moment in time. A lot more research and development needs to be put into that particular area. I have also seen further increases in security options available on the handset itself by certain manufacturers. The facilities are there, but I have not seen them being used in the main at this moment in time although that could possibly change as time goes on.

Q157 Mr Malik: To what extent are the problems you face created by the volume of data available on, for example, calls made and received?

Mr Parmar: As far as the call history data is concerned, that is usually not historic, that is going to be pretty much current and it is going to be a small amount. For example, normally you are looking at 10 missed calls, 10 received calls and possibly a maximum of 20 dialed calls that can be obtained from a device. Is that data accurate? No, you cannot rely on that information just from the device itself, it has to be corroborated by a billing record to confirm that those calls were successful.

Q158 Mr Malik: So the volume is not a major issue is what you are saying.

Mr Parmar: No, it is relatively short and it has been for a number of years.

Mr Smith: It is the interrogational interpretation of it that takes the time.

Q159 Mr Malik: If there was twice as much resource within the police service to deal with this issue, would it be dealt with twice as quickly?

Mr Smith: I think the problem is not chucking money at it. I do not think the problem is trying to find 24 personnel. I think the issue is providing the right skill sets and experiences they need to deal with it. The problem is that there is a dichotomy between what the law enforcement agencies are asking for and what they do through their training centre of excellence which they have just started with mobile telephone courses. How that would impact on them getting the job done quicker we think would be negligible. It is the skill sets that are missing and the experience, it is not the production line bang it on, bang it out type of effect.

Q160 Mr Malik: How widespread are the skills needed in telecoms forensics?

Mr Smith: I think it has to be subject specific. If somebody has telecommunications experience coming into the wireless domain, which we are, then that is useful and the same would be quite right to say for computers. I think you need the discipline in the subject that you are dealing with and then to have the others use those other skills and to bring them together so you get a symbiotic relationship.

Q161 Mr Malik: Are you a rare commodity? Is there enough of you out there?

Mr Smith: The answer is no. Vinesh is one of the highfliers in this country and so is Daren. I have the longest track record in this country in dealing with mobile evidence.

Q162 Mr Malik: Can one expert direct a team of less skilled assistants in this area of work?

Mr Parmar: Certain organisations, not just law enforcement agencies, will have key people in key areas. They usually split the process up. When it comes to telecoms, they will have those that specialise in the data recovery process and those that specialise in the presentation analysis of that process. In some areas those processes will be split

plus you will have a third element where there is somebody that is proficient in all areas. I believe that in order to be able to be in a position to do this type of work successfully you need to understand all the elements. You do not have to be an expert in all elements, but if you have an understanding of all elements and choose a specialist area then you should be quite successful. That is the view that law enforcement and other organisations need to take when they are recruiting and training their personnel.

Q163 Mr Malik: Are there resources that the police have not called on that might make their work easier?

Mr Parmar: It is not a question of not utilising resources, it is a question of the police understanding what it is they require. Too often we get requests which say we want everything, which in reality is not a workable request. What we find is that law enforcement agencies need to start understanding the data that is available and to start understanding what is possible evidence or what is intelligence and they need to split it and make valuable requests to us so that we can do the best job we can. At the moment a lot of work we do is fishing expeditions where we are basically requested to grab everything out of there and we do not know the case history.

Q164 Mr Malik: Are there external organisations that could assist the police that are not being engaged at this time in your view?

Mr Parmar: At the moment the law enforcement agencies do utilise the resources that are out there.

Q165 Mr Malik: So to your knowledge it is not really an issue at the moment, is it?

Mr Parmar: No.

Mr Greener: If I could answer that, I am often instructed by defence solicitors and therefore on many occasions I go into police constabularies throughout the country to audit the work that has already been done by the prosecution. Going back to a previous question about the level of resource, it is often found that that level of resource does not match the resources which are outside the Police Service or is not at the same level of competence. It is often the case that a particular person who may be skilled in one particular package is used to examine a phone and things like that. I have had a number of conversations with various police officers and detectives at various times who say that they would like to use our skills but they do not have the authorisation to commission us to do any work themselves. It is often already pre-arranged at a contract level at some stage, so as an outside organisation we are excluded or we are not utilised and requested.

Q166 Chairman: Can I just check one thing for my understanding? What I think you are all saying to the Committee is that the challenges here are not actually the handset issues. The challenge in terms of

14 February 2006 Mr Daren Greener, Mr Vinesh Parmar and Mr Gregory Smith

understanding and analysis is the records from the phone companies of the calls made and so on. Is that broadly right?

Mr Smith: Broadly speaking that is correct.

Q167 Gwyn Prosser: Mr Smith, you know our inquiry is trying to put together the estimate of time taken in particular cases with the 90 days which the Government wanted to put in place as pre-charge detention. When you were answering questions to Mrs Cryer you started telling us about pin numbers and access blockers et cetera, and you said that of course you had had a lot of these in some particular cases. I think you said in the worst case scenario that could take a long time “but we are not talking about that; we are talking about the general run-of-the mill case”. But we are not here; we are talking about those particular cases which can have huge ramifications and might take 90 days. In that context, in the same way as Mr Sommer earlier on said that yes, there could be rare occasions when the work of the computer forensic people might take up that full 90 days, is that your view as well with regard to your technology?

Mr Smith: Yes, I would say that is quite correct. There is a section where, if you allow an individual or an individual is smart enough to put all the passwords and identity numbers in place, you can have on the 3G up to 16 different passwords which would take you a long time to crack. Most people do not bother; that is the truth of the matter, so 90 days, yes, but I think that must be scrutinised very carefully as to the reasons for that.

Q168 Gwyn Prosser: But perhaps a determined terrorist might bother.

Mr Smith: I would not say they do not. I do not know. All I can say is that I think it is a balance.

Q169 Gwyn Prosser: Mr Parmar, we have heard a lot of criticism and qualifications about the way the police use this technology. Would you say there is a need to re-assess the whole approach to telecoms forensics?

Mr Parmar: Yes, I believe so. I believe a lot more resources and a lot more training and awareness have to be put into it for those who are involved in this type of work to understand exactly what they are doing and what they are responsible for. I think there is a general lack of understanding in that respect. What I do find—and this is no criticism—is that generally law enforcement will send the people who are responsible for this type of work on two- or three-day courses and no further training is offered. I do not believe that is a correct approach. I believe that it requires long term investment and long term resources just in the training to make sure that the people who are doing this type of work are up to date with current practice and current technology.

Q170 Chairman: Would you know if that applied as much to specialist parts of the Police Service with largely anti-terrorist work as it would to general policing?

Mr Parmar: I am not just making references to specialist areas or to general practices. It is not just applicable to law enforcement; it is applicable generally to all those technicians that do this type of work. There does not appear to be a mechanism in place where certain skills have to be attained throughout a certain period of time. Greg will back me up on this as a trainer, as to whether there is anything official about that.

Q171 Chairman: You may not know the answer to this question, in which case say so, but would you say that those who specialise in anti-terrorism investigations have similar weaknesses in the way in which they approach telecoms analysis as you see in the Police Service generally?

Mr Parmar: Are you making reference to the people involved in terms of doing this type of work?

Q172 Chairman: Yes, because obviously the starting point for our inquiry is that the police are saying to us, “We need 90 days because various parts of our investigation, which may include telecoms analysis, take a long period of time”. You have made some very important points about the general quality of the police understanding mobile telecoms issues. It is obviously relevant to this Committee to know whether those weaknesses are shared by those police officers who would be responsible for counter-terrorism investigations.

Mr Parmar: I do believe there is an element of weakness there, but as to what quantity I could not comment.

Q173 Gwyn Prosser: Mr Greener, some witnesses have argued that the length of time that telecom data is held should be increased by legislation. Would you support that?

Mr Greener: I would very much support that. The existing legislation is at best historic data for 12 months, and one element that we have from the data is the ability to track historically people’s movements or whereabouts at a particular time. In cases where we are conducting this type of cell site analysis, as it is termed, tracking where the mobile phone placed a call according to the various masts that are run throughout the country, if we are talking of a large network of phones which produce that sort of pattern that in itself takes a period of time and a lot of survey work and a lot of mapping work to produce that. It is often quite a way down the investigation before you find other phones that are coming into the fold, as it were, and therefore they require separate analysis in themselves, so 12 months’ retention of that, for both the purposes of the prosecution and then afterwards therefore the defence to verify various things is often not long enough. On that basis of cell site analysis it can be the case that I am instructed some 12 months after the incident date and therefore there is not any further extended record in relation to that cell site and the movements of those particular phones.

Q174 Gwyn Prosser: What about the standardisation of call data?

14 February 2006 Mr Daren Greener, Mr Vinesh Parmar and Mr Gregory Smith

Mr Greener: Yes. We have mainly have four network providers, all providing call billing data or cell site analysis data. There is a variance between those operators in terms of the level of detail that you get to work on, to analyse, so a standardised, across-the-board output would be beneficial to the analyst and would also minimise the skill set slightly across all analysts so that the data was understood by one and all.

Q175 Gwyn Prosser: Are there any other gaps in legislation which you would like to see filled?

Mr Smith: No, I think we already have it. The biggest problem that people have with legislation is that they do not bother to read it. Therefore, if they do not bother to read it or try to get some interpretation of it, they misunderstand it and they go on from that misunderstanding to make a mistake.

Q176 Gwyn Prosser: I am talking more in terms of legislation which would be beneficial to forensic analysis.

Mr Smith: Oh, I apologise.

Mr Greener: For me, where we have discussed the legislation to extend the retention of the data, standardisation across that data would certainly be beneficial, but I cannot think of changes to the existing legislation further than that.

Mr Parmar: I cannot see any issues with the current legislation.

Mr Smith: Not at all with the CP Rules coming out, by the way.

Q177 Mr Winnick: Mr Smith, in answer to Mr Prosser you said that there may be instances where the police require the 90 days to get the information. Would it not be also the case that you could say that the police require more than 90 days? If they require up to 90 days in certain instances, presumably very exceptional, the same surely would apply, would it not, to the argument that the police require double that amount of time in very complex cases?

Mr Smith: There is always the potential for that to arise. It would be wrong to say otherwise.

Q178 Chairman: I am going to put to Mr Greener and Mr Parmar a question that Mr Smith has answered about whether from your knowledge of mobile telecoms issues and the analysis of them you personally think that the pre-charge detention of up to 90 days can be justified by the complexities involved in doing telecoms analysis.

Mr Greener: I think the 90 days will allow more time to galvanise the initial evidence that we are working with and to analyse it thereafter from the existing 14 days that I believe it is to gather in the phones.

Q179 Chairman: Are you saying that on the basis that there are things that you simply cannot do within 14 or 28 days that you think are necessary to support a charge?

Mr Greener: I am basing it on experience in cases where phones are being brought into the investigation along the way, so it is the gathering of evidence period.

Q180 Chairman: Thank you. Mr Parmar?

Mr Parmar: It is going to be based on the amount of items which have been submitted for examination. If it is a large volume then the current timespan is probably not going to be enough, so therefore I would welcome a 90-day extension to give us that opportunity to look at every possible device that has been submitted. My experience dictates that in particular high profile cases we do not just receive one or two devices, for example. We see possibly 30 or 40 different individual items to look at and that takes a considerable amount of time.

Q181 Mr Winnick: Why 90 days, as I put the question to Mr Smith? Why not longer?

Mr Parmar: The 90 days would give us more time to deal with the request as opposed to having to deal with a 30-day request when it comes to examining, say, 30 different items.

Q182 Mr Winnick: But if you had 180 days that would be even more time, would it not?

Mr Parmar: There is that, yes.

Chairman: Gentlemen, thank you very much indeed. It has been a very useful session.

Tuesday 28 February 2006

Members present:

Mr John Denham, in the Chair

Mr Richard Benyon
Mr Jeremy Browne
Colin Burgon
Mr James Clappison
Mrs Ann Cryer
Mrs Janet Dean

Nick Harvey
Steve McCabe
Mr Shahid Malik
Gwyn Prosser
Mr Richard Spring
Mr David Winnick

Witnesses: Assistant Commissioner Andy Hayman QPM, Metropolitan Police Service (MPS), and Deputy Assistant Commissioner Peter Clarke CVO OBE QPM, Head of the MPS Anti-Terrorist Branch and National Co-ordinator of Terrorist Investigations, gave evidence.

Asterisks denote parts of the oral evidence taken in private which, for security and legal reasons, have not been reported at the request of the Metropolitan Police Service and with the agreement of the Committee.

Q183 Chairman: Good morning and thank you very much indeed for joining us at this further evidence session into the Committee's consideration of the case for extended pre-charge detention. We are very grateful to you for coming and for your evidence. I wonder if each of you could just introduce yourselves briefly for the record.

Assistant Commissioner Hayman: Andy Hayman. I am Assistant Commissioner for the Metropolitan Police with responsibilities for Specialist Operations which include the Anti-Terrorist Branch and Special Branch.

Deputy Assistant Commissioner Clarke: Good morning. Peter Clarke. I am Deputy Assistant Commissioner in the Metropolitan Police. I have two roles, if you like: one is as Head of the Anti-Terrorist Branch in the Metropolitan Police; and, in addition to that, the Association of Chief Police Officers has given me the role of being National Co-ordinator of Terrorist Investigations, which means I have a national role in terms of that particular function.

Q184 Chairman: Thank you very much indeed. We look forward to drawing on your knowledge and expertise this morning. Obviously the proposal for up to 90 days' pre-charge detention is one of the most controversial criminal justice changes there has been for some time. I would like to start if I may by asking some questions about the development of the policy of detention for up to 90 days. So far as the Committee was able to establish, in the autumn the main communications that the Government received from ACPO arguing for 90 days consisted of three press releases and two sides of A4 describing a couple of operations. I wonder if either of the witnesses could take us through the process that ACPO went through to come to the conclusion that up to 90 days was necessary.

Assistant Commissioner Hayman: In terms of the process, Chairman, we will try and do a double-act because we have both got contributions to make. So

we get a bit of variety, one will lead and the other will follow-up after that. Perhaps on that one I will lead and Peter can add whatever he feels is relevant. First of all, I think it is worth stating at the outset that an invitation by government for an opinion is not unusual. With a different hat on, that happened last year around the Drugs Bill. In my other role as Chair of the ACPO Drugs Committee I was asked for an opinion and we went through that normal consultation.

Q185 Chairman: Could I just stop you. That is very interesting. It may just be me but I had understood that the proposal for extended detention up to 90 days was one that was made from ACPO to the Government unsolicited, as it were. Are you saying that actually the Government invited views on a further extension beyond the 14 days?

Assistant Commissioner Hayman: As it does with other agendas, the Government invited views on the subject matter, the question being posed.

Q186 Chairman: Specifically on detention or on general terrorism?

Assistant Commissioner Hayman: No, on general terrorism legislation. It was occurring around the time of the atrocities in July. Quite rightly, there had been deliberations before that but it became more focused in the wake of July. Discussions between government and other agencies, not just the police, were in a consultative phase. It was a professional view about: what is working well; what needs to be revisited; and where are the gaps? The way in which that consultation was instigated was in many different forums. There is a statutory consultation home affairs working group which is with the Home Office and also within ACPO. As you would expect, having been given that invitation ACPO as an association then consulted its members and were asking those questions, exactly as we would do with any other agenda. When it comes to the specifics which you have asked, Chairman, around the 90 days, I think what needs to be clarified fairly strongly here was that the proposal from ACPO was that we felt from experience and investigations (matters which Peter can add more detail to) that 14 days was not sufficient and we were looking for an extension. This is a real subtlety which needs to be underlined.

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

The extension proposed and suggested by ACPO would always be in line with any human rights legislation, and that would be subject to a judicial review. What then became a debate and discussion point was, how long can this go on for; how long do these judicial reviews keep occurring for? ACPO were being pushed for a judgement on that—and it was no more than a professional judgement—which is 90 days. What I think has happened on reflection is that the 90 days dominated the discussions and considerations, when actually the proposal was for judicial extensions.

Q187 Chairman: Can I take you further. This Committee certainly appreciates the subtlety you are trying to point us to there. ACPO though had obviously concluded that 14 days was insufficient. Could you tell the Committee how ACPO came to that conclusion? Did ACPO do what I know it has done on other issues in the past and set up a working group, professional group or study group to produce a report and analysis for internal consumption and then reach the conclusion; or was there just a view amongst officers working in this area that more than 14 days was necessary?

Assistant Commissioner Hayman: I will refer in a minute to Peter because he was obviously instrumental in helping us come to that view, but it was all those things. A letter was sent out to all ACPO colleagues across the country asking for views by the then Chair of the ACPO (TAM) which was Ken Jones, Chief Constable of Sussex; and material was then brought into a central point. It was very much influenced by Peter's world on the experience of investigations. Before I refer to Peter on this—the real difficulty here (which I know members are very alert to) is that the material (and we have got material and we have original material here) is difficult to share. That is the dilemma which we have currently got. We would be delighted to share it under certain circumstances but it is very difficult.

Deputy Assistant Commissioner Clarke: If it would help the Committee, I could perhaps put an operational context on this and where the thinking came from.

Q188 Chairman: What I would like to know, without going into the detail of the cases at the moment, is how the case was assembled and what process of analysis was actually gone through. In the autumn when we as a Committee enquired what exactly had ACPO sent to the Home Office to justify its support, it came out of three press releases and two sides of A4. It did not look like a particularly substantial document of the sort we might have expected would have existed at least in confidence. I am very interested in how ACPO came to the conclusion that 14 days was inadequate?

Deputy Assistant Commissioner Clarke: What I can do is tell you how officers working with me in the Anti-Terrorist Branch on terrorist investigations all the time came to that conclusion—not through working groups, not through documents, but

through discussion over a period of time and using what we saw as evolving trends from casework to inform our judgment. So when the time came last summer and we were invited by the Government to put forward any measures which we felt would be useful in terms of amendments or new terrorist legislation, the proposal for extended detention was one of those issues we put forward. It was not the subject of a formal working party within the Police Service prior to that. It was the product of a lot of discussion and reflection by practitioners over a period of some two to three years. Remember, of course, that back in 2003 we had had discussions with government which had led in January 2004 to the extension from 7–14 days, and that was in response to trends we had seen emerging which had been set out in the paper which Mr Hayman sent to the Home Office in October—those trends we had seen back in 2002 and early 2003. The extension which was 7–14 days then was very welcome. What we then saw during 2004 was an acceleration of those trends with some specific cases which again (as Mr Hayman has said) I am in some difficulty in going into detail on because they are currently *sub judice*. Those cases really showed us the features which we set out in the paper to be continuing and developing features, and that is why we put forward the 90-day proposal.

Q189 Chairman: That is helpful. I am remiss and I will say something now that I should have said at the beginning and this is for the benefit of members of the public. I have indicated to the witnesses, given the nature of what we are discussing, that there may be a point in this morning's evidence session at which we invite the witnesses to give us evidence in confidence if there is evidence which cannot be used in public session. It may be that we will return to some of these matters later on in this particular area. Obviously for everyone's benefit we want to deal with as much as we possibly can do in public and on the public record. If I could go back to the process, I am right in thinking that it is very common in ACPO if there is a new policing problem to be dealt with for ACPO to go and set up a group of professional experts who produce a report, a business case for change. That was not done in this case. Why was it not done on a matter of such great importance? Terrorism is obviously important; civil liberties are important; why did ACPO not do what it has done on so many other issues before, which is to convene a proper professional working group to come up with recommendations?

Assistant Commissioner Hayman: I would just change that slightly, Chairman, because there are cases where the rigour you have just described is appropriate but, equally, I can cite other examples, and I have used one already which is the Drugs Bill proposal, where that was not the case and the proposal caveated that way. Government has asked for a professional opinion and that is what it has got. If you want a more substantial case which is

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

describing the features you have, the rigour features, then quite clearly we will do that, but that was not the question that was asked.

Q190 Chairman: The position as far as we perceive it: ACPO put out a press release I think in late July or early August saying that they would like to have more than 14 days' detention up to a maximum of 90 days; by the middle of August the Government had decided to back the ACPO request. Did the Government ever ask for any more evidence or exploration of the case for more than 14 days than has been made available to this Committee in the form of ACPO press releases and the two sides of A4?

Assistant Commissioner Hayman: No.

Q191 Chairman: Were you surprised that the Government was prepared to back an extension from 14 days to up to 90 days on the basis of, yes, a professional opinion but so little analysis of the alternatives, how it might work in practice, the international experience and so on?

Assistant Commissioner Hayman: Clearly that is a matter that needs to be addressed to the Government.

Q192 Chairman: It will be, but as a professional police officer were you surprised, having put the initial position that you would like up to 90 days, that the Government did not come back and apparently say, "Well, possibly, but let's have some chapter and verse on this"?

Assistant Commissioner Hayman: An honest answer to you, Chairman, is: no, it did not cross my mind at all. I think there are some other very interesting comparisons where other periods of time have reached the legislative framework—the amount of hours for detention after review under PACE 24, 36 and 72. How did we reach those hours? It was the same sort of rigour you have described attached to that. You can go into other periods of time, not just in this profession. The answer to the question is: no, I was not surprised; and, secondly, it would be very interesting to explore how those other days were reached in other legislative frameworks.

Q193 Chairman: Indeed. The Prime Minister was quoted, I think in October, not long before the parliamentary vote with saying there was incontrovertible evidence in favour of the need for up to 90 days' extension. Are you aware of any information given to the Prime Minister other than what went in the two pages of A4 and the letter you yourself sent later in the process?

Assistant Commissioner Hayman: I can comment on that. I personally attended in the wake of July (and I can remember it very clearly), before the Prime Minister went away on annual leave, personal briefings along with other Security Service colleagues of the emerging picture. I do not know whether that is what the Prime Minister was drawing on. All I can say is that information had been shared.

Q194 Chairman: I do not want to put words into your mouth but just to make sure I have understood what you are saying, from an ACPO point of view, from your position as a professional police officer, the need to go more than 14 days is something of which you are absolutely certain. The question of whether the maximum period should be 90 days is much more a sense of instinctive judgment about what feels about right. Is that fair?

Assistant Commissioner Hayman: That is absolutely fair. I know that sounds pretty flaky. I expect members are sitting here thinking, "Crikey, there should be more basis for that", but that was the question that was asked. It is a really difficult judgment call to make, but we were asked for a professional judgment and that is what we gave. I want to go back to the earlier point, that we would not see this was being the norm. This is about an extension for detention before the 14 days with judicial oversight.

Q195 Mr Winnick: Mr Hayman, given there are no Members of Parliament, to my knowledge, who do not recognise there is an acute terrorist danger to our country, and that would be the position and was indeed the position before the atrocities of 7 July and what may or may not have happened a fortnight later, were you at all surprised that a large number of MPs were not persuaded that the 90 days was justified?

Assistant Commissioner Hayman: I have never formed a view on that. You now pose the question and I will try and give an intuitive reply. I am never surprised really; people have got their own views. It is not for me to do anything other than present as much information as I professionally can to form a debate and it is for others to form their own opinion. I am not so sure that the question about whether I am surprised or not helps out. You can never judge how people are going to go when they see all the information.

Q196 Mr Winnick: But it did come as somewhat of a surprise to you?

Assistant Commissioner Hayman: I guess the only thing I am left asking is: on the basis of the information that is available and the level of threat, and if the professionals have been asked for an opinion, I would have hoped we would have had the integrity (when we came to the table for that opinion) to be trusted as I would do if I went to see a surgeon or any other specialist or professional. I guess I am left asking the question of whether or not we were convincing enough in presenting our argument.

Q197 Mr Winnick: You are making the point that if you went to see a specialist you would expect to accept the specialist's point given to you. Are you therefore saying we should have accepted the 90 days because the police suggested it?

Assistant Commissioner Hayman: No, I think you are pushing me into a position I am not actually arguing.

28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM

Q198 Mr Winnick: I am taking it from what you have just said.

Assistant Commissioner Hayman: I am saying that the professional body was asked for an opinion and we gave that opinion. Members have weighed that up against what they feel and what other information they have got and they have individually come to a decision which is the real democracy in this country. I just felt information that was presented started to make a fairly compelling case that said beyond 14 days there was a case for further detention with judicial oversight. If others who have got to vote on that do not feel that way then that is a matter for them.

Q199 Mr Winnick: Mr Hayman, is there not a possibility, a pretty strong possibility, that members took into consideration that the increase from 7 to 14 days had been in operation for less than two years, and now it has been in operation for just over two years? Do you not consider that would have been a pretty serious consideration that the police had been given the extra powers which had been in operation, as I say, for less than two years?

Assistant Commissioner Hayman: Of course, what we have seen happen in the passage of those two years across the world and the complexity of the attacks and the atrocities that have occurred means that the timescale of two years becomes irrelevant. If it had been two months and there had been a massive change in circumstances, to be not flexible enough to change one's opinion or review legislation would be remiss.

Q200 Mr Winnick: Another factor which perhaps you can confirm is that what came out in the debate is that no-one who had been held in detention and then released (and I emphasise "released") had later been charged with terrorist offences? Is that not the position?

Assistant Commissioner Hayman: It is the position.

Deputy Assistant Commissioner Clarke: Yes, that is exactly the position.

Q201 Mr Winnick: That is the position. Let us get it absolutely clear—no-one who has been held in detention under the powers given to the police and then released has later been charged with terrorist offences?

Deputy Assistant Commissioner Clarke: That is absolutely correct.

Q202 Mr Winnick: Mr Hayman, it is said in the paper that the police have given us that "extensions past seven days are used very infrequently". But more than one in 10 of those arrested under the Terrorism Act 2000 had been held for longer than seven days pre-charge; and between a quarter and a third of those suspects were released without charge. Can I therefore ask you, what proportion of suspects would you have expected to be held longer than 14 days if Parliament had agreed to the request, and how many of them would then have been released without charge?

Assistant Commissioner Hayman: It is a tall order to come up with an analysis like that. What I am saying is I am very proud of the investigations that are bound to operate without the constraints of the 14 days, and have been able to gather evidence under extreme circumstances to not go beyond that guillotine. What I am saying, and we have always said this in our oral and written submission, is that regardless of what timeframe we come up with for future proposals, we would see this as being a very extreme set of circumstances where it is going to occur. What we do know from our investigation is that it is a tall order to get within the 14 days.

Q203 Mr Winnick: Finally, on reflection do you not think you would have been much better to have stayed with the 14 days and, recognising the statistics which come from the police, the case for a longer period could have been put before Parliament later than it did do, namely less than two years since the 14 days had been in operation?

Assistant Commissioner Hayman: You have mentioned that twice, and I am struggling to understand the relevance of why it is just the two years; because with the world events and those that happened in this country (and you cannot ignore that this became a pressing government priority in the wake of the atrocities) there needed to be a point of reflection and review. Whether it was two years or two months becomes irrelevant.

Q204 Mr Winnick: But the initiative came from the Government?

Assistant Commissioner Hayman: We answered a Government question.

Q205 Chairman: How many of those that you have released without charge over the last couple of years do you believe you would have been able to charge if you had detained for longer?

Deputy Assistant Commissioner Clarke: That is a question that has been asked on many occasions and, if I may say so, Chairman, I do not think it is the right question because we do not know. It is a statement of the blindingly obvious: we do not know what we do not know and we cannot guess at what might have occurred had we been able to keep people longer. I am in no doubt whatsoever that in several cases there have been instances where the evidence would have developed to a stage where charges would probably have been more likely, certainly where intelligence would have flowed, and I can only speculate but a lot of this is speculation, where there could well have been instances where public safety could have been well served by some of the information that could have come from a longer period of detention. This is not I hasten to add solely about interviewing people. A lot of this is about having the time to properly investigate the information and the evidence which emerges in these cases. You have seen the papers which explain the whole range of issues which now make it more difficult and which make it necessary for us to have longer. There have been cases where I am quite sure

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

that there were people who had been arrested as part of a broader group who—had we had the opportunity to fully understand their particular role within the conspiracy, had we had the opportunity to serve that on the defence and for them to be in a position to recognise that we recognised their particular role—might well have chosen to say more to us or to say anything to us.

Mr Winnick: Mr Clarke, that could be an argument for much longer than 90 days, because before we knew where we were we had agreed to 90 days and in another year or two years you would be selling us the same position: if only we had more time, and therefore we require 100 days or 140 days and so on and so forth?

Q206 Chairman: Mr Clarke, please continue to answer the question because there is a key thing here that we need to get, which is the people who have been released you feel we might have done more with.

Deputy Assistant Commissioner Clarke: I have been asked to identify which terrorists have evaded justice—I cannot do that. What I can do, and I am not arguing for more than 90 days, I am just saying that on the trends which we have seen develop in these investigations over the past three to four years there is, to my mind, no doubt whatsoever that the changed nature of the threat, the global nature of the threat, and all the other characteristics which we now see which we did not see in the past mean that on any calculation we need more than 14 days to be in a position to have sensible constructive interviews, to fully understand the nature of the conspiracies that we are looking at, which are global and complex. As Mr Hayman has said, I do not think there is any magic about 90 days. What we are asking for is a longer period beyond 14 days and it is not a police power—that is a point I would like to emphasise.

Mr Winnick: But you are getting it.

Chairman: There is an issue about 90 days *per se* but it is also very important that the Committee understands, if you like, the underlying case for extended detention.

Q207 Mr Spring: We read your hypothetical case study and it obviously does reflect to anybody who reads it the sheer complexity and difficulty that you face in these cases. We absolutely understand that. Tim Owen QC made some comments and criticisms of this particular case study and if I could just remind everybody of one or two of the points that were made. For example, that the threat itself has been greatly exaggerated; but also that it proceeds on the assumption that at the point of arrest police have literally no evidence and that the 14 days provides the only opportunity to commence investigation, and he disputed that; also that at the point of charge the CPS must in effect serve all its evidence, whereas in fact in practice he asserts that the CPS have effectively about six months to do this. Two final points: bail is hardly ever granted in terrorist cases; and also, finally, and I think this is a

point we do need to examine, the benefits of interviewing from his assessment point of view is greatly exaggerated. Trying to balance the complexities as you have set out, which we all understand and appreciate, and these criticisms, I just wonder how you react to the points that he has made in trying to demolish your particular case?

Assistant Commissioner Hayman: If I deal with the points about the nature of the threat and the issue around bail, and then I will refer to Peter on the other issues. We read Mr Owen's comments with interest and it has to be said, as a headline, I do not actually agree with those points. First, to be saying that we have greatly exaggerated the nature of the threat I do not see that there is a basis for that statement at all. In fact if you look at events around the world, if you look at the autumn there was an unprecedented period of about three weeks where we saw attacks in Bali and Delhi, thwarted attacks on Australia and London, and that was in a very short space of time with loss of life. If we look at the threat levels set around the world that just flies in the face of us saying that it is an exaggerated threat. I do not see there is a basis for that at all. In relation to bail, I am not quite sure how the judiciary and the criminal justice system would welcome those comments, because actually that is not a question that should be levied towards the police—that is a question levied to the judgment and the operation of the judiciary. I can tell you, I do not see it as a walk in the park. In the history of going before a court or the officers at the moment going before a court, to ask for remand as a custody or whatever, that is certainly not a walk in the park. On those two points I just do not recognise them.

Deputy Assistant Commissioner Clarke: The point about the case study being based on an assumption that the CPS had all or would need all the evidence at the point of charge, I am afraid I do not recognise that at all. Of course there never is all the evidence available at the point of charge. These cases take many, many months to construct and develop the evidence and make those enquiries overseas. At the point of charge the CPS have to have reached a stage at which they are satisfied it is appropriate for the charge to be levied; and that is very different, of course, from the stage at which an arrest is appropriate. In order to make an arrest one merely has to have grounds—and that could be based on intelligence, it could be based upon material that is not admissible in court. Indeed in one particularly significant case which is awaiting trial, at the moment we arrested the people who now stand charged with very serious offences there was not one shred of admissible evidence at all; but on grounds of public safety we felt obliged to intervene at that stage and to make the arrests. Over the subsequent 14 days, intensive work led us to the point where on the fourteenth day the Director of Public Prosecutions felt able to authorise charges in respect of those people. It is not based upon the assumption that you have to have all the evidence at that stage. I am sorry, the other two points were?

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

Q208 Mr Spring: He talked about bail hardly ever being granted in terrorist cases and also (something I want to come onto) interviewing, and we can come on to that.

Deputy Assistant Commissioner Clarke: In respect of the bail issue it is a fact that there is no provision for bail under the Terrorism Act, so it is not something which can be granted.

Q209 Mr Spring: I think we can all agree that at the heart of this is the efficacy of the interviewing process—that is just absolutely key. We took some evidence in this Committee from Lord Carlile and I would just like to indicate two things that he said. He talked about the interviewing process being “rarely productive”; he also said, “. . . in my view, the interviewing process is actually becoming not entirely irrelevant, but near to irrelevant”, and we all know why, because of the right to silence and the advice which is given to individuals to remain silent. I am not sure we understand the difficulties which flow from this. Taking this particular point of Lord Carlile’s, which was indeed confirmed to us by other witnesses, and given the fact that in many terrorism cases these individuals will remain silent, what are the implications therefore for a prolonged pre-charge detention, given the fact that it does not seem to work in practice other than the suggestion which was made, I think, by Mr Clarke that people may be persuaded to talk if it was made clear to them that their role was a minor one in any particular potential terrorism case and finally to allow them to gather evidence. I think this is a very important issue which we need to be clear about in our minds.

Assistant Commissioner Hayman: The point I would make is that any detention is not just solely for interviewing—it is for gathering the evidence that will probably form part of an interview strategy. The point made by Lord Carlile is well made, but that does not mean to say we should assume someone is not going to talk to us and we must not deprive someone of the opportunity to actually make comment when evidence is being presented to them. For me the time of detention should not just be focused on interview, albeit that is the most critical part of it; it has got to be around the development and gathering of evidence to that charge.

Deputy Assistant Commissioner Clarke: I can foresee circumstances in which, after an initial interview to ascertain whether or not somebody wished to explain circumstances to us, we might not wish to interview somebody for perhaps days or even weeks because the gathering of the evidence, which is catered for within the legislation, might not be through the medium of an interview. It could well be through analysis of telephone or computer data or enquiries made overseas. Then we might want to return and put that material to the person who has been arrested. Under the proposed provisions under the Terrorism Bill it may well be if somebody is remanded into prison custody from police custody we would then have them produced back into police custody towards the end of that period of detention to enable us to put to them the things which we have

been able to find in the intervening period. It is terribly important, and I agree with Lord Carlile entirely, that the efficacy of the interview process is comparatively small. We have recently conducted some research and found that in Anti-Terrorist Branch cases well over 60% of people detained do choose to exercise their right to silence. We broke that down a little further into those who are considered by the investigators to be either leaders or supporters, as a broad categorisation, and we found that only one in 10 of those who would be considered to be leaders or directors of terrorism chose to speak.

Assistant Commissioner Hayman: This example has been ridiculed by some commentators, but I will go back to it and if we do go into a private session I will be able to give you much more material to support this point. If we had a scenario post 7 July where there were survivors from the attackers and they were in custody, in terms of investigation of where we saw the bomb factory and the amount of time it took to get in there with safe entry and actually analyse what was there, it would take us well beyond 14 days or any other time period you might want to describe. Therefore, we know we want to speak to X because we have linked X to the scene but we cannot speak to that person; and the point Peter is making is that we would not want to prematurely anyway, and we would need to wait until we were in a position where we were ready to discuss the matters with that person. When we go into the private session we can give you more information on that.

Q210 Chairman: It does sound though, and this may be what is coming out, that the primary aim of detaining people is actually preventive—in other words, to prevent them continuing planning terrorist activity—far more than actually doing anything with them that enables you to charge them?

Assistant Commissioner Hayman: It could do. I have read Lord Carlile’s evidence to this Committee and there is one particular point where he described different scenarios which I support. The scenario could be on the basis of public safety and early interdiction to prevent an atrocity which could occur and that person would be detained, and that would fit into what you have just described. On the other hand, down the chain of events there might be a much later interdiction where there is evidence to be gathered which is very resource-intensive where there are much more substantial things to interview, which goes beyond a conspiracy. With the new legislation that has been proposed within the Bill for acts preparatory to terrorism that will probably become more the norm than we are seeing at the moment.

Q211 Mr Benyon: I want to talk about the more practical constraints and the difference of opinion that exists between the hypothetical case that you produced and opinions on it expressed to us, particularly in this case, by one of the solicitors, Ms Peirce, from whom we heard. In the scenario you talked about the importance of interpreters and that

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

this is a constraint when you take a suspect into custody, and that you need an interpreter as soon as suspects are brought into a police station after being arrested. Why do you point to the need for interpreters as a cause for delay when suspects are later interviewed? Is there really such a difficulty in finding predominantly Arabic interpreters?

Deputy Assistant Commissioner Clarke: You have to take the issue of interpreters along with all the other factors we have put into the submissions around why it is that, taken together, they contribute to the lengthening of the process. In terms of interpreters, yes, there is a lack of availability of interpreters, not only because of the language issues but of course dealing with this sort of material they have to be security-cleared as well. Remember, it is not only the process of the police station we need our interpreters for. There will frequently, for instance, be eavesdropping material which they have to transcribe and translate for us. There will very often be hundreds of documents seized which have to be translated for us so we can then analyse them before putting them into an interview strategy. We have seen in several cases where suspects have come from some fairly remote parts of the world and the need not just for Arabic interpreters but for some people who can interpret in dialects which very few people speak. Indeed I can think of one case in the not too distant past where we actually had to bring an interpreter in from the other side of the Atlantic to assist us because there was no-one available in this country who could do that for us.

Q212 Mr Benyon: One of the other constraints brought out in the hypothetical case that we had was that there was a delay because a multitude of people had been arrested and there was only one firm of solicitors that was acting on their behalf. Ms Peirce disputed this. She said there were many firms who had the expertise and the wish to represent these people. Would any solicitor seek to represent a client in your experience if they could not do so properly? Her argument was that your hypothetical case was not made and there were plenty of people who were able and willing to do it and there should be no time constraint as a result?

Deputy Assistant Commissioner Clarke: I have to say, I do not recognise Ms Peirce's analysis of that situation at all. There are a limited number of firms who specialise in this area of work—Ms Peirce's firm is one. In this open session I cannot go into some details but I would say to your question of whether, in our experience, there are solicitors who do not represent clients to what we consider to be an acceptable professional standard the answer is, yes, I have seen that. I think there have been occasions when what anybody else would recognise as clear conflict of interests have arisen through multiple representations of clients by one firm, and of course that is not a matter for us as police officers to point out to those professionals—that is a matter for them to recognise themselves. I would say undoubtedly there have been occasions when the representation

afforded to people has not been of the highest standard because of this multiple representation issue.

Assistant Commissioner Hayman: Can I just clarify one point. There was a hypothetical example in the paper and when we get into a different session you will see on a scale of one to 10 it is probably hitting about seven, and I can see real cases of *sub judice* which will go beyond that.

Q213 Mr Benyon: The other point is that in the hypothetical case you have to make allowances for frequent periods of religious observance, for Muslim prayer. In your experience is this really a factor in terms of limiting the amount of time that you can interview a suspect because they have to break for prayers four or five times a day?

Deputy Assistant Commissioner Clarke: I would not honestly say it is a factor which interferes with the amount of time that is available for interview. I think what it is, it is something we have to take into account when we are setting out our investigation and interview strategy; and we have to factor in breaks and proper opportunities for prayer to take place. It is difficult to quantify, but I would put it forward as another issue which we have to take into account when looking at the overall time available for the investigation to be completed in a proper fashion. We cannot just say, "Right, we'll set aside X number of hours for interview on a particular day", because we have to make sure there is proper opportunity for religious observance built in. So I would not want to quantify that.

Q214 Mr Benyon: My last point—and I think the most serious criticism that Ms Peirce gave to us—is based around the physical constraints of Paddington Green, in most cases. Despite an enormous amount of money being spent on Paddington Green (and no doubt it is a very secure place to hold suspects) she argued that it has an entirely impractical layout to interview people in a timely fashion; a limited number of interview rooms; difficulty with access. She also criticised the Anti-Terrorist Branch for an over-methodical process of evidence-gathering and progressing an investigation. I am quite convinced you have got strong views on that, but we have been told that suspects are not interviewed very often during the first 48 hours in detention; and that only 10% or less of the time a suspect is detained is used for interviews. In relation to that and her criticisms, how would you reply to that?

Deputy Assistant Commissioner Clarke: It is a pleasant change to be accused by Ms Peirce of being over-methodical! In terms of the facilities at Paddington, yes, this is a secure unit which was built in the 1970s and early 1980s. I would be the first to say that I would like us to be able to move to somewhere probably more suited to the scale of cases and the number of suspects we are now seeing in the modern era. We have spent a lot of money on upgrading it. There are now more interview rooms; there are three interview rooms there. We are doing what we can to make it as amenable an environment

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

as possible, particularly bearing in mind now the possibility of people coming back after 14 days' detention. In terms of the suggestion that we do not interview for the first 48 hours, I am afraid I do not recognise that either. There is no policy about that. Indeed, it is very often in our interests to have an interview as soon as we reasonably can so that we can get an indication of an individual's intentions and demeanour in respect of the investigation. I simply do not recognise that. If need be we could supply all sorts of custody records and the like to the Committee which would show that that is simply not the case. Yes, interviews are structured; of course they are. We start off usually with basic information about an individual to build up a picture of that person before we start moving through a process of staged disclosure of material to defence. That is entirely appropriate; it is a proper investigative strategy. You do not put all your cards on the table at the very beginning, you stage the disclosure. Indeed in many of these cases we stage it as the material becomes available to us through all the other strands of enquiry which we are pursuing in parallel with the interview process. In terms of the amount of time that is actually taken up during detention by the process of interview, of course since the advent of tape recording some 20 years ago the process has become much shorter now. So what used to take several hours of handwriting to record an interview now can be done in a matter of minutes. I do not have the exact details but what I do know is—from some survey that has been done about the total amount of time taken for interview in relation to the overall time in detention—that the upper limit we have seen is about 20% of time taken up for interview; but that is at the top end and I think a more reasonable estimate is probably somewhere between 10 and 15% of total time on detention actually taken in the interview process.

Q215 Mr Clappison: We have heard evidence about proposed alternatives to the course which you favour, and we have also had some evidence from yourselves about that. Could I ask you about one or two points on the alternatives. You say that greater resources would not tackle the basic problem of the weight of material and the need for it to be analysed; but would it not be the case that greater resources would help in some respects, as for example where you were analysing large volumes of data or where you were looking at opportunities for interceptions of communications?

Deputy Assistant Commissioner Clarke: I was asked this very question by the Joint Committee on Human Rights last autumn and I think my answer is still fundamentally the same. That, yes, while obviously the greater resources in the initial gathering stage for data would be and always are useful, and of course we put whatever resources are required into that stage of the process, gradually it filters down and the process is sequential. If I could give an example—it would be gathering telephone data. If you go into premises to search them a thorough search will normally take two to three

days. During the course of that search nowadays we regularly find large numbers of SIM cards, mobile telephones and the like. That material has to be recorded *in situ* and it has to be taken to the laboratory and the material downloaded from it. Then the investigation has to move onto the service providers to gather billing data and the subscriber details. That material then in turn has to be recorded and analysed, and that has to be put into the interview strategy to try and work out where that fits into the context of the overall investigation. That is essentially a sequential piece of work. The same applies to lots of other parts of an investigation. Recovering fingerprint data from documents, for instance, is a sequential thing; it just takes time. Examining the chemical analysis of materials found in premises of explosives and the like does take time. I am saying, at the initial stages, yes, have the broad brush; throw resources at it; but then when you get the material you have to start focusing it down. What we have found is not good practice is to have too many people engaged in the final analysis of material before it is fed into an interview strategy, because if you have too many people they will not have an overall view of the investigation and might not recognise the significance. One example in one particular case was where we did try to bring in extra people to wade through computer material over the course of a weekend, but because they were not fully sighted on all the issues in the particular case, they actually missed a vital piece of material on a computer hard drive, which was only thankfully then recovered by one of the detectives who had been engaged in the whole case and was able to see it. The point that I am making is that you have to narrow it down eventually.

Q216 Mr Clappison: You are saying in short that it would be a help to have more resources but that does not remove the need for a longer period of detention?

Deputy Assistant Commissioner Clarke: Absolutely not.

Assistant Commissioner Hayman: Too many cooks spoil the broth.

Q217 Mr Clappison: Another alternative which has been raised and which has been part of the debate is potentially charging suspects with lesser offences. It is right to say you have raised a number of legal difficulties with this and also the risk of diverting resources. It is also right to say that Lord Carlisle set his face against charging suspects with lesser offences at an earlier stage, and it does look unattractive in some ways. Are you saying that there are no cases in which that would be a useful way of proceeding, to charge someone with a lesser offence?

Assistant Commissioner Hayman: I just think this is so unpalatable. It is unfair; it flies in the face of true justice. What are you really going to gain from that? It is surely the case for an investigation to gather the evidence that is available to prove or disprove someone's culpability in a criminal offence. The notion of us trying to basically get round the

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

problem of longer detention by bringing in a lower level charge is just not acceptable professionally; and I do not think it is fair to the suspect either.

Deputy Assistant Commissioner Clarke: If you are going to charge a lesser offence you have got to have the evidence, for a start that might not be available.

Q218 Mr Clappison: You mention that in your written evidence.

Deputy Assistant Commissioner Clarke: Of course it would always be open to the person to plead guilty and ask for the case to be disposed of by the courts and that would be the end of that particular ruse, as is being suggested it could be termed as.

Q219 Mr Clappison: One of the other alternatives which has been mentioned generally in this debate is the use of control orders. Do you feel they are appropriate to be used in these cases?

Deputy Assistant Commissioner Clarke: Personally I do not think so, no, because we are only talking about applying to the courts for an extended period of detention in respect of the most serious cases right at the top end of the investigative scale—those people who potentially provide the most serious threat to public safety. To suggest a control order, which is designed for an entirely different purpose, as an appropriate way of safeguarding the public against the sort of people we are suggesting should be subject to extended detention during the investigative stage, I do not think that provides sufficient reassurance for the public or indeed the level of protection for the public that is appropriate.

Q220 Mrs Dean: Following on from that with control orders, could terrorist conspiracies be disrupted by the use of control orders and tagging, linked with the existing periods of pre-charge detention?

Assistant Commissioner Hayman: Disruption is always a tool in the kitbag. The measures you have described are always going to be useful. We must not lose sight that the cases we are describing, which are born out of the debate around the period of detention, are the ones that have gone beyond that, and they are probably going into the preparatory acts to make an attack. That is well evidenced in the investigations where we are waiting to go to trial over the next two to three years. I have just got to be really careful. I understand what you are saying. They are a very useful tool in the kitbag, but they are not appropriate for the circumstances we were arguing around detention.

Q221 Mrs Dean: You are generally supportive of allowing post-charge questioning. Can you give examples of cases where you would have still wanted to be able to detain suspects for 90 days pre-charge, even if post-charge questioning was allowed?

Assistant Commissioner Hayman: We have never said we wanted to keep them for 90 days. It is a subtle point but one which has to keep being made, I think.

Q222 Mrs Dean: Up to 90 days.

Assistant Commissioner Hayman: There is a case which was cited by Lord Carlile in his evidence which is one I rely upon which would have been helpful.

Q223 Mrs Dean: Do you think that once charged suspects would be less inclined to speak because they have no incentive to do so?

Assistant Commissioner Hayman: It is a good question. Who knows, because they are not always going to talk at the start, are they?

Q224 Mrs Dean: You mentioned difficulties with providing intercept material of an evidential standard as a problem with allowing its use in courts. Could you give examples of such difficulties with foreign intercept material which is allowed in court?

Assistant Commissioner Hayman: This has been a fascinating discussion over a fair amount of time and I speak from an ACPO and personal perspective. I have personally moved my position. I originally started off by being fairly unsupportive of the notion of using the material, mainly on the basis that it was starting to disclose methodology to the other side. I think that is now well and truly worn-out because I think most people are aware of that. It does not stop them still talking but they are aware of the methodology so that is a lightweight argument. The next point which I had reservations about was the true logistics about transcribing the material, where you could go into reams of material. Again, that is a fairly moot point now, given that you can be very selective about the things you are going to transcribe if you are very precise on your investigation and focused. I think I am moving, as I know ACPO is, to a conclusion that in a selected number of cases, not just for terrorism but also for serious crime, it would be useful. I think also it does make us look a little bit foolish that everywhere else in the world is using it to good effect.

Q225 Chairman: Could I just take you back to the exchange with Janet Dean and James Clappison about control orders, where the answer was essentially that these are very dangerous people and, therefore, not having them locked up is not sufficient security to the public. Does that not bring us back to the earlier point that actually your main case for extending detention is actually to disrupt or prevent terrorist activity, as opposed to having more time in which to gather evidence?

Assistant Commissioner Hayman: I was reluctant earlier on to support that point, but as the debate has matured in here I can see where you are coming from on that. There are a vast amount of cases now where an early interdiction is to disrupt on the grounds of public safety. What we are hopeful to do is to gather evidence that would culminate in a charge. Unfortunately, at the moment as we stand without the new legislation being in place, ie acts preparatory to terrorism, sometimes it is really difficult to make

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

that fit what is on the legislative books. With that new legislation, with the early interdiction, yes, I can support your point.

Q226 Gwyn Prosser: Mr Hayman, on the issue of intercept evidence, are you saying that ACPO are on the brink of recommending to ministers that there should be a change in legislation to provide intercept evidence in exceptional cases?

Assistant Commissioner Hayman: Of course we will provide a robust business case behind it in relation to that because, given we have to change our position, that is required. The problem we have still got is that in about 18 months to two years' time there is going to be a change in technology, which needs to be borne in mind. Certainly if we are asked a question, that is what our response would be.

Q227 Gwyn Prosser: Mr Clarke, you have told us this morning the amount of evidence required for a charge is a great deal more than that required for arrest. I suppose we should expect that to be self-evident. In evidence we took and opinions we elicited from JUSTICE they said there should be greater attention given to the Threshold Test in section 6 of the Code for Crown Prosecutors. They went on to say that that would allow the CPS to bring charges on reasonable suspicion, which is the same as the test required for arrest. What is your view on that?

Deputy Assistant Commissioner Clarke: The application of the Threshold Test is something which the Crown Prosecution Service has to answer for themselves. But if I may offer my observations on this: the CPS still has to have evidence in order for a charge to be preferred. It is totally different from the grounds for arrest. The CPS is not allowed to speculate as to what evidence may become available in the future. The Threshold Test is there for them to be able to prefer a charge where bail is not suitable, but where the standard for the final test (the realistic prospect of conviction) has not yet been reached; but they are allowed to take into account that evidence which they can reasonably anticipate will become available during the course of the investigation. So I think there is something of a red herring about this, because I do not think the Threshold Test is at all applicable in these sorts of cases. It is not that we are saying to the CPS, "This is what we've got, and this is what we think we'll get"; this is in cases where we have not got sufficient to charge and require more time, or are asking for more time to actually go and find the evidence which is not yet available and we do not know is there. It is an entirely different concept, and I do not think the Threshold Test is something which really plays into this debate at all.

Assistant Commissioner Hayman: A good example which was given to me—and forget the case because they are not comparable—if you imagine a very routine shoplifting case where you know you will need certain statements to support the prosecution but you just have not got those, that is when the Threshold Test is applicable, when it is a matter of

going out and getting those statements to add to the case. As Peter says, you just cannot compare that with a terrorist investigation.

Q228 Gwyn Prosser: A number of witnesses also told us that using Part 3 of the Regulation of Investigatory Powers Act would be helpful in avoiding long periods of detention before charge. What is your view on that?

Deputy Assistant Commissioner Clarke: Is that in respect of the encryption debate?

Q229 Gwyn Prosser: Yes.

Deputy Assistant Commissioner Clarke: The provision within Part 3 has not yet of course been implemented. I think it is important to bear in mind, if it was to be implemented, that would carry a penalty of two years' imprisonment. What we are looking at here are people who have secreted or encrypted material on their computers who, if that material were to be found, would stand the possibility of perhaps facing 20 years' imprisonment. If the choice is between giving the key to us to find evidence which could potentially lead to them serving 20 years or refusing to give the key to us and potentially being liable to two years' imprisonment under Part 3 of RIPA, I think the choice is fairly clear which one you would take. I think what we need to do is we do need to think about what sort of encouragement we could give to people to release the encryption keys, but I think the way to that is probably to find some way of aligning the potential sentence more closely to the ultimate offence, if you like, or that offence which perhaps, if we could show there is reasonable grounds to suspect an individual was concerned with it, would be the one that they were charged with, but for the fact that they were refusing to release information. It is a difficult area because it gets into self-incrimination issues and all of this, but I do not think Part 3 RIPA, as it stands, if it was implemented, would be the answer to it.

Q230 Steve McCabe: I want to ask what I hope are some fairly straightforward questions about computers which is probably a big feature in this. As you can imagine, I am a computer buff. In your judgment, do you have the resources both in terms of equipment and personnel that you need for decryption and other computer forensics?

Assistant Commissioner Hayman: The use of computers not just in terrorism cases, but also in serious crime, bank fraud, et cetera, means that not just the Police Service, but wider industry, commerce, et cetera, are all hunting the same skill-set, so, although we still need conventional and traditional detective investigative skills, they need to be complementary with what we call "hi-tech crime skills", so we are actually all competing for the same limited amount of resources. You get into market forces to see who can pay the best buck to keep the people and what we do find is that it is not necessarily the job of a police officer, a warranted officer, but that could be done by a non-warranted

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

officer. Whilst we can end up training people to do certain skills, there is a level of retention which, for all of us, is an issue. I need to make the point that the actual encrypting of these computers is not necessarily something that the Police Service would conduct, other agencies would do that, but typically, when we are looking now at the growth that we require, there will be a balancing act between those conventional skills and the hi-tech crime skills.

Q231 Steve McCabe: How often do you come across encrypted material and can you give us some idea of the average length of time it might take to decrypt material?

Assistant Commissioner Hayman: I will ask Peter to answer the second part, but I think the better question to ask, and the answer to the first question, is: when do you not? Rather than how many times, it is when do you not.

Q232 Steve McCabe: It is extremely common?

Assistant Commissioner Hayman: Well, it can be as basic as the password right up to something very sophisticated where it takes weeks for a machine to decrypt it.

Deputy Assistant Commissioner Clarke: I think there are two issues. One is about encryption itself which, as Andy says, some of it is just password protection, and another is commercially available software which can, as I understand it and I am no expert on this, lead to some deep encryption which can take a long, long time to answer, to break. Indeed I have seen in the United States a computer left running for weeks on end to try to break through encryption. The other aspect of this is of course hiding material which takes time. What we have seen is, for instance, a DVD of a film and the officers sit down to go through this film and, about an hour into the film, suddenly it changes into a terrorist targeting video of locations, so that again is an issue which takes a considerable amount of time. Just because someone has got a set of commercial films does not mean that is what is actually on them, so we have to go through them and we have found material, which has formed the subject of charges, buried in that way.

Assistant Commissioner Hayman: I think our nightmare scenario, regardless of where we are coming from, on length of detention or anything like that, surely has got to be what on the face of it appears to be a very innocent, innocuous piece of material which then means that someone is not arrested or is released and then weeks down the line suddenly becomes a horrendous revelation. That is the nightmare scenario.

Q233 Steve McCabe: Is it common for unencrypted material to lead to a charge by itself?

Deputy Assistant Commissioner Clarke: It has done, yes. I can think of some instances where we have recovered things, such as I can think in one particular case, and I am treading carefully because it is *sub judice*, where we recovered what is virtually a 25-minute film of how to make suicide vests. Now, my understanding is that that was not actually

encrypted, though I am not sure whether that was hidden within the computer system, but I do not think it was encrypted, as such.

Assistant Commissioner Hayman: My understanding is that it was not, that it was on a pen-drive which had been downloaded off a hard disk. Again I am treading carefully and I am only speculating, but it may be that the suspect was just a little bit haphazard then in not having the sort of back-up of the security of encryption, but who knows.

Deputy Assistant Commissioner Clarke: We have seen cases as well where people have thought that they have managed to delete things from their hard drives, but actually they have not been able to clean them entirely and we have been able to recover material.

Q234 Steve McCabe: I was just thinking, we took evidence the other week from some computer experts, which you may have seen, but what takes the most time? Is it the decryption of material or is it the analysis of the material?

Deputy Assistant Commissioner Clarke: I would probably have to ask my own computer experts, but I think they would tell me that it is the analysis of the material. The decryption, we send off elsewhere for that to be done, and it depends upon the depth of the encryption as to how long that takes and whether it can be achieved at all. There are some things which in one case I can think of, which is two years old now, where we still have not been able to access all the material.

Assistant Commissioner Hayman: What that does is, and it is a statement of the obvious really, but once you start to understand what the material is telling you, it then leads you into, because you go wherever it takes you, it leads you then into associations with people and other networks and that then will lead you to other material which you need then to interrogate. Typically, we could show you on office walls the print-outs of association charts and linkages which all develop into lines of enquiry which again have to be managed in a very meticulous way.

Q235 Steve McCabe: I think Professor Anderson suggested that analysis was almost infinite or at least until the analysts got fed up with it. Is that your view as well?

Assistant Commissioner Hayman: I hope it is not when they get fed up with it, but certainly that is a tall order for them, yes.

Q236 Steve McCabe: Finally, it is pretty evident that the growth of computers, I guess, in all sorts of investigations is a serious issue and it must pose questions about the police management strategy. I just wondered whether you could say something about how your management of inquiries has adapted to try and accommodate this new system or new approach?

Deputy Assistant Commissioner Clarke: Yes, it really does play into the whole discussion we are having this morning about the shape of an investigation.

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

Traditional, good detective work is that you follow the evidence wherever it takes you and that is the purity. You keep an open mind from the beginning of an investigation and follow the evidence where it takes you. However, with the weight of material we are now seeing, what we actually have to do is to set clear priorities at a very early stage and we have to make choices around which material we are going to try and access on computers or through mobile phones or overseas and hope, and it really does come down to hope, that that will yield the evidence we need prior to the end of what is now the 14-day period. As I described earlier, in one case it was on day 13 that the nugget came out of the computer system, so, if we had chosen a different hard drive to look at, we might not have found that at all and the people who now face very serious charges would have had to have been released. I think that is the key thing. The other part about the management of the investigation is the weight of resources that you put into different aspects of it, so, whereas in previous times we might have perhaps focused on forensics, for instance, and put a huge amount of resources into that, now increasingly we have to try and focus it on the analysis of technological data. There is an example of the importance of this, and again I must be careful, but there is one case which is now coming before the courts where what we will be alleging is that this is the first instance in our experience of a virtual network where we will be saying that there are people who have conspired together to commit terrorist acts, but they have never actually met, or we have no evidence at this stage of them having met other than electronically, so that perhaps gives a flavour of the sort of shift in the nature of these investigations and I hope that is helpful.

Assistant Commissioner Hayman: There are two points I would add to that, I think. There is that description Peter has just given of that allegation which has very strong rings in paedophilia crime, and again we know the challenges that has been presenting in recent years. I was just reflecting when you asked that question and I think I would want to go further than that. I would just look at the technology that is now available to us all and it is conceivable that I could walk out of my home with a throw-away mobile phone, with a couple of SIM cards and I could have two conversations with you using different SIM cards, or I could communicate with you through a PSP and, if I wanted to be really careful, I would go to an Internet café and use different terminals in there. I could probably have a conversation and contact with you, having walked out of my home and come back, where conventional surveillance was a waste of time and, even with technical surveillance, it is a challenge because of how quick I am changing the medium through which I am communicating with you. Therefore, when we get to the bottom of that, we have to go back to where I started when I went out of my home with those two throw-away mobile phones and went to the Internet café. I just think the complexity of that should never be underestimated.

Q237 Colin Burgon: You have mentioned mobile phones and I noticed in the Metropolitan Police Service paper accompanying your letter of 5 October that you said that the use of mobile phones by terrorists as a means of secure communications is a relatively new phenomenon. Do you think you have, in the case of this new phenomenon, the necessary resources both in terms of equipment and personnel to handle this whole issue of mobile phones?

Assistant Commissioner Hayman: Yes, and it is not just of course the Police Service that contributes to the investigation, but it is other agencies that do. I am certainly not going to use that as an opportunity to pitch for more resources because I think what has been given to us at the moment is sufficient. The earlier points that Peter made that we do not just sprint at this and we have to be very methodical, too many cooks spoil the broth, I think, is a good way of describing that. I also think we need to be very measured in the way in which we start to develop our own strategies to deal with this. We have got to see how these things start to unfold. Is the mobile phone going to be redundant in a couple of years' time? For the moment it seems to be the main way of communicating. There is one particular case of allegations here of over 300 mobile phones with about 140 SIM cards, so in that particular case it is suggested that that was the main medium, but it may not be. What I do not think we should be doing is responding to what we see as being a problem now and we have to try and get ahead of the game here and try and identify what the new medium will be and then bring in strategies to deal with that.

Q238 Colin Burgon: With regards to your relationship with the network providers, we had an expert witness tell us, for instance, that, if it is a level one incident, an immediate threat to life, then usually they can let you know what you want within two or three hours. How important are, and how can you develop, these relationships with the network providers which seem to us, as outsiders, to be absolutely crucial?

Assistant Commissioner Hayman: Well, I would not want to go into too much detail here, but I think the headline would be that we are blessed with very good relationships, very professional, where the balance between the libertarian perspective and the subscriber as against the need for investigating the serious crime of terrorism is struck, in my view.

Q239 Colin Burgon: The expert that we listened to said something, and I would like you to respond to this. He said that the police or the people in charge who are responsible for this type of work send people on a two- or three-day course and then no further training is offered. Is that an accurate picture of your training of officers in relation to mobile phones or do you think it is a bit unfair?

Assistant Commissioner Hayman: I think the description is modest. By the time you have registered and had lunch over a couple of days, there is no input, is there? That would just be ridiculous. I think we would look at it as being a much longer

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

period of training and of course, once you are involved in investigations, you develop your expertise in the field.

Q240 Colin Burgon: But you would agree that long-term investment and training are needed to ensure that officers keep up with the pace of technology?

Assistant Commissioner Hayman: Yes.

Q241 Colin Burgon: Is that a resource issue because I noticed earlier that you said you were not pitching for resources all the time?

Assistant Commissioner Hayman: We feel that the level of resources that we have got, certainly the Government's recent new money which has been allocated not just to the Police Service, but all the other security agencies, is sufficient and it is for us now to deliver outcomes which we have said we will be able to do.

Colin Burgon: I am sure the Home Secretary would be delighted to hear that!

Q242 Mr Browne: Mr Hayman, carrying on on the same theme, would you expand on the point you just made about the balance to be struck with mobile phones between the liberty of the individual user, if you like, and the access and the co-operativeness that you get from the phone operators?

Assistant Commissioner Hayman: As you know, the legislative framework demands certain thresholds to be met in terms of intelligence and any kind of intercept, or whatever else you are alluding to, maintains those levels of threshold. There is nothing you can do to bypass that, so, unless those things are in place, it is not a conversation, and I would say that is what you rely on.

Q243 Mr Browne: But you find that the phone companies understand the scale of the work that confronts you, that you do not feel you are constantly having to justify access in a way that is frustrating to you?

Assistant Commissioner Hayman: That is not even an issue.

Q244 Mr Browne: We have just spoken for the last half hour or so about technological requirements, whether it is computers or mobile phones, but is there a frustration for both of you that Parliament, when considering this 90-day detention period, does not fully grasp or the public do not fully grasp how technical by nature a lot of this investigative work is, that there is a conventional idea of an interview process where you follow the evidence and you have the experience and police officers who have got a lot of track record in this record has been overtaken by a far more sophisticated process where you are looking for needles in haystacks the whole time and that the legislation is not keeping up with that? Can you think, for example, of particular cases where just the technical requirements, leaving aside everything else, would in themselves justify keeping someone for three months just because of the sheer amount of material you have to sort through?

Assistant Commissioner Hayman: If we go into a different session, I can certainly share that, and maybe we have not made it strong enough, but in the early submissions and in the debates which went on in the summer/autumn, I know I certainly gave an example where the hard drive had been seized and, if the material had been printed, it would have equated to 66,000 feet of paper piled up and it is only luck obviously if you find the relevant material when you first start the interrogation of that material. If you got to the 65,000th foot, you would be really unlucky, would you not? I think, and this may be completely pie in the sky, but I do think the general opinion of the public is informed by what they read and what they see in different mediums and, therefore, if they are informed by popular TV shows which depict investigations and that show, obviously because it has been focused more on entertainment than anything else, does not go into what we see as reality, that is the way in which public opinion is formed. I am not making a judgment about that, I am offering a commentary and I might be wrong, but, if that is the case and the majority of people are informed by what they read and what they see, from what I see and what I read, it bears absolutely no resemblance to what I see and experience every day at work.

Q245 Mr Browne: So, rather than having some Miss Marple figure who sort of comes to this amazing conclusion, you actually really need dozens and dozens of technical men and women, sitting there, sifting through acres of material and that is the changing nature of investigation?

Assistant Commissioner Hayman: Yes, we are building at the moment a new response to counter terrorism as part of our restructuring and we are looking at the functionality that is going to be required. I guess the breadth of the coverage that we now need in terms of skills profile is just unrecognisable as to what it would have been even five years ago, so the point I was making in answer to questions was that we are just desperate to try and get ahead of the technology and that is why we are working with the industry to try and understand what the technology is going to be in five to six years' time so that we can start preparing for it in our own plans now rather than the sense, it has to be said, that we are always trying to play catch-up.

Q246 Mr Browne: Mr Winnick right at the beginning was saying, "Why stop at 90? Why not have 100 days, 120 or 140 days?" That is a reasonable point and I am not trying to lead you to an answer one way or the other, but, if you have 66,000 pages of evidence to go through and it gets even more sophisticated and even more complicated, would it be reasonable to say, just from a straightforward crime prevention point of view even if you leave aside for the moment civil liberties, that there may be periods where even 90 days is not sufficient to go through the amount of material you need to in order to reach the nugget that Mr Clarke talked about?

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

Assistant Commissioner Hayman: Maybe, maybe not. We are going back into the sort of previous discussion where we were asked for a judgment and, on balance, three months. I would start to get an uncomfortable feeling if it goes beyond that, it is unreasonable. You have focused on the fact that that is the only line of enquiry we had available to us for that investigation, in which case it would be difficult to get it maybe in 90 days, but one would hope that there are other lines of enquiry which are there and, if they are developed, would give you grounds for charging or disposing in another way and you would not just have to rely on that 66,000 feet of paper.

Q247 Mr Malik: I would just say that the interference we heard earlier on was my phone and it was a text message from the Home Secretary who says, "Thank you, Mr Hayman"! On a serious note, I think a thank you is owed to you, to the Met, and in particular to the way you have co-operated and worked with West Yorkshire, my particular constituency, which had Mohammed Sidique Khan who was the leader of the suicide bombers. I think we are all grateful to you for the work you have done and the work you are doing. You talked earlier on about trusting your integrity and opinion and I voted for 90 days, whereas the majority of my colleagues here did not, but I think we all trust your integrity irrespective of which way we voted on that particular point. The question really is about the current system of judicial oversight of pre-charge detention. There is this kind of accusation that really it is some kind of rubber-stamping exercise because it is the prosecution who alone present their case to a judge to authorise the extension. Do you think that the current system can be fairly described as robust or is it indeed this kind of rubber-stamping?

Assistant Commissioner Hayman: Peter is probably more appropriate to answer that from his perspective, but I have gone on public record many times, saying that this is just unfair, this is not a walk in the park. You go in front of a judge and, regardless of your view on the case, the judiciary have got a role to play and they are very probing in their scrutiny of the evidence and, if anyone thinks this is a nod and a wink to get through that process, I think that is an insult both to the judiciary and ourselves.

Deputy Assistant Commissioner Clarke: Just to build on that again I do not recognise the expression "rubber-stamping" in respect of the process of the application for warrants of further detention which is gone through. This is a very meticulous and detailed process and, most importantly, it is an adversarial process. The suspects are represented in court and the case is argued out in front of the district judge, so to suggest that somehow that then is a rubber-stamp, I find strange. Again, when I was giving evidence here before the Joint Committee on Human Rights last October, I was asked if I could recall any occasions on which our applications had been rejected. I could not then, and I cannot now,

recall one where the application in totality was rejected, but I can think of many occasions where we have asked for perhaps four or five days and the district judge has said, "No, you have 48 hours. Come back after 48 hours and show us what you have done with the time which the court has granted". These whole issues are looked at with great care, in my experience, and I have talked to district judges about this informally and they are utterly robust in their examination of the cases put before them. I think also the fact that we have not had total rejections of our applications for warrants of further detention is an indication not of rubber-stamping, but it is an indication of the care with which we put those applications together always in concert with the CPS. We always consult with the CPS, we examine the material, and we discuss with them whether an application would be justified and, if it is not, we do not make the application. It is as simple as that.

Q248 Mr Malik: It has been put to us by previous witnesses that evidence obtained from a person who has been held for, for example, more than seven days in custody would not really be taken into consideration by an English judge and certainly not that which is longer than 14 days. The question really is: how confident are you that pre-charge detention for more than 14 days would be consistent with the European Convention on Human Rights?

Deputy Assistant Commissioner Clarke: Having seen that evidence that was given previously, we took counsel's opinion ourselves because obviously this is a matter of some legal technicality and I think there are two issues which flow from counsel's opinion which we have. First of all, the cases which were cited to this Committee as suggesting that periods of detention actually for less than 14 days were incompatible with ECHR, counsel tells us that those cases are not authority for the proposition that 14 days' pre-charge detention with appropriate judicial involvement is incompatible with the European Convention, and the key point there is judicial involvement. Of course we have to go before the district judge after 48 hours to apply for a warrant of further detention and I think it is a key point that is often missed in this discussion, that this is not a police power, this is a judicial power exercised on application by the prosecuting authorities, so counsel's opinion on this is that this is not incompatible with ECHR so long as there is appropriate judicial involvement. Then on the question about the admissibility of evidence obtained after 14 days, again counsel says that those cases which were cited to this Committee are not relevant to the question of interpretation of evidence obtained after a lengthy period of detention and counsel makes it absolutely clear that you have to take the entire context into consideration, and that would be a matter for the tribunal of fact, ie the court, to decide whether or not evidence can be relied upon.

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

Q249 Mrs Cryer: Can I seek further clarification on the questions that Mr Malik has put to you. We had a witness, Mr Owen, before us earlier this month and he observed that he found it difficult to see how the average English judge would regard it as fair to admit evidence obtained after a person had been held for more than seven days. Therefore, do you think that evidence obtained after a person has been held for longer than 14 days without charge is likely to be admissible in an English court?

Deputy Assistant Commissioner Clarke: Again this is clearly a matter for some legal debate, but, if I may quote a sentence here from counsel's opinion on this very point, he says, "So long as the detention is lawful and there has been no oppression or unfairness, there will be no reason to exclude evidence obtained after 14 days merely because of the time when it was obtained. The weight which is to be given to it will depend on all the circumstances of the case". That is the best and the current opinion which we have from counsel.

Q250 Mrs Cryer: So you disagree with what Mr Owen said?

Deputy Assistant Commissioner Clarke: Well, it is not for me to agree or disagree with learned counsel; it is for me to say that we have sought advice on this because clearly this is an important matter that was brought before the Committee, so we have taken legal advice ourselves so that we could discuss this with you here today.

Assistant Commissioner Hayman: It must be stressed here that we have got two separate counsel offering different opinions on a set of circumstances, which is not unusual!

Q251 Mrs Cryer: Can I also ask both of you for your views on the dangers to community relations arising from someone being released after a long period of detention without charge and, when you were preparing your submission regarding the request for 90 days' detention without charge, did you seek information from, for instance, Colin Cramphorn, who is the Chief Constable of West Yorkshire where the young men came from involved with the bombing? Did you ask his opinion due to the fact that he would be left keeping the peace during the 90-day period?

Assistant Commissioner Hayman: Colin is a very well-respected colleague with experience in working in Irish terrorism cases, so he would be someone clearly we went to. I think it is a wider point really. I think the issue of our relations with all sections of the community has got to be at the heart of all of our work, whether it is following detention or whether it is following investigation or trying to actually prevent. One of the things we know, because we have responded, hopefully in the public's opinion, in a very positive way, is that we have put a lot more effort and a lot more resources into developing better community ties, particularly with the Muslim community, but actually I would not want to single out that community over and above any other. Success for us has surely got to be a greater

transparency and openness without contravening any kind of confidential material where the community understand what we are doing and why we are doing things, so there is, therefore, an acceptance of the need to do it rather than things being very sort of secretive where people do not understand why things are occurring which then causes conflict. I think that is a very, very important point that we have to have very much in our minds.

Q252 Mr Winnick: When it came to the debate, or just before the debate itself, in November and prior, what was the position of ACPO in contacting or encouraging senior police officers to contact the Member of Parliament in a particular area?

Assistant Commissioner Hayman: Certainly I am aware of the letter that was sent by the Chair of TAM, Chief Constable Ken Jones. I cannot recall the exact detail of it, but my recollection of its tone was that in those circumstances where Members of Parliament wanted more information to understand the detail of what was being submitted, then that might be an option for local chief constables or local commanders to avail themselves for that kind of briefing. Certainly the intention, as is my understanding, was to do nothing more than to give the opportunity for as much information to be available to enable people to inform their own opinion so that they can respond accordingly.

Q253 Mr Winnick: So how did the process work? Did the senior police officer in a given area phone or leave a message for the Member of Parliament to contact him or her?

Assistant Commissioner Hayman: I do not know. I guess whoever responded to that would react in different ways. I would imagine that most, if it was a divisional commander or a chief constable, would have very healthy, productive relationships where it would not be amiss for people to be contacted by phone or in person and maybe that is what happened. On the other hand, maybe that did not.

Q254 Mr Winnick: Would you describe that as a sort of lobbying of MPs?

Assistant Commissioner Hayman: No.

Q255 Mr Winnick: How would you describe it?

Assistant Commissioner Hayman: As part of an ongoing relationship that I always enjoyed when I was the Chief Constable in Norfolk where, having a relationship with my local Members of Parliament, it would be inconceivable not to avail myself for opinion not just about that subject, but about the wider subjects, whatever they might be. For us to be in a position, Mr Winnick, where we were concerned about having conversations with Members of Parliament on any particular topic, be it ahead of a vote or ahead of any other debate, I think would be a retrograde step.

28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM

Q256 Mr Winnick: Do you feel that, on reflection, it might have been counterproductive that Members of Parliament, rightly or wrongly, came to the view that pressure was being put on them?

Assistant Commissioner Hayman: Did you feel that then?

Q257 Mr Winnick: Do you think it was counterproductive, what actually happened, in the sense that some MPs, perhaps not many, nevertheless felt there was some pressure which was being put on them to vote according to what the Government wanted?

Assistant Commissioner Hayman: I was not being disrespectful when I posed that question because I cannot speak for other people, but I can ask you that question. If you feel that way, I can then have a conversation with you about it, but I cannot second-guess other people.

Chairman: Colleagues, as I indicated earlier, we are now going to move into private session so that we can now go through some of the more detailed information that has been offered to us.

Q258 Chairman: There were a number of points during the session where you wished to refer, or you said it would be helpful to refer, to specific investigations and I think it would be useful perhaps if you could give us what illustrations you can of the number of points which have come up in the evidence. There is obviously the general point, if you like, about the dangerousness of certain suspects and the reason for detention and then perhaps you could then look at some of the reasons for particularly lengthy delays in getting evidence.

Assistant Commissioner Hayman: Well, what we have prepared for you in anticipation of this is one side of A3 and, if it is okay, I would like to distribute copies, if that would be helpful, and that will be a script which Peter and I will work through. What I will do is I will try and give you a general overview of what has been presented here and then it is probably appropriate if Peter just gives a flavour, a couple of features which seem to sort of appear in every investigation and then it is over to you, Chairman, and members as to what they want to probe. What this starts to paint for you, I think, especially if you look at the timescales from 2002 through to the current time, is the sort of span, the breadth, the depth of investigations into terrorist activity. Some of the material is seized very quickly, some of it is not seized for some time and in the vast majority of these particular cases we can cite, certainly within the 14-day period, which is obviously the key focus for us all here, the material was seized. It does pose the question in terms of logistics, regardless of how many resources you have got and personnel already, of to what extent you are able to get a grip of what actually has gone on and who is actually involved. For example, if you look further down the page, ***, February 2004, in that particular investigation who were we actually speaking to because there were 860 passports and a number of identity cards? When you then look at the amount of exhibits that existed in

***, all right, that is obviously the second part of July, but there are 45,500 exhibits there. Again, if you look at the fingerprints, the number of fingerprints there in the top, Springbourne, there are 1,600 fingerprints and, okay, they are all pretty relevant, but how long does it take to lift a print and analyse it? Well, it is a considerable amount of time just for one fingerprint. In summary here, and we can go into more detail, what this is trying to describe to you is the depth and breadth of investigation that is challenging for the individual investigators.

Deputy Assistant Commissioner Clarke: What it shows, I think, as well is the development which has led us to the conclusion that the trend is such that we need the extended period of detention. If we go back to Springbourne at the top there, this is the so-called "ricin investigation", it was unprecedented in its scale in the number of countries it took us to, the number of forged documents and all the rest of it that went into that, and that began our process of thinking that really we are looking at something here which is unprecedented in terms of criminal investigation. That led us to the discussion, as I said earlier, with the Government about the need to go to 14 days. ***.

Q259 Nick Harvey: These figures, are they all relating to what you and the British police have done? If they are in lots of other countries, are they augmented by further numbers in various other countries?

Deputy Assistant Commissioner Clarke: Yes, this is what we have in our system here as part of our investigation. Then Operation *** in August 2004, which is a bit further down, this was a case which really caused us to think again and you could say this was the case which began the thinking around the requirements for extended detention. This was a case where we had intelligence that there was a group of people in the United Kingdom who were engaged in terrorist-planning of some sort, target unknown, methodology unknown. We managed to identify them, but their trade craft, for want of a better expression, was good and it was at such a level that we could not keep control over that group through surveillance to the level that we felt was required for us to be sure that public safety was not at risk. We did not know how far their planning was advanced. *** This was the case I referred to where there was no admissible evidence at the moment of arrest. We started recovering all these computers and in the subsequent 14 days I had officers sleeping on the floor, not going home at all, just to try to get into this huge amount of material. It was on the very last day that the DPP authorised charges and now there are eight people charged with conspiracy to murder, conspiracy to cause explosions, conspiracy to cause a public nuisance in terms of irradiation and the like. After that, we sat down and said, "Well, how are we going to deal with this sort of case in the future?", and that was when we began to think about the sort of features that were playing into modern terrorist investigations and giving us cause to think of how

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

within our current system we could do this. It really drove us to the conclusion that we would not be able to even within the 14 days because the trend was becoming clear through Springbourne, ***, ***, and that trend has been carried on with *** at the bottom, which is the case I referred to of the virtual network. That promises to be an even bigger investigation than the previous ones. It is still in its early stages, ***

Q260 Mr Clappison: Can you just take us back to *** which you mentioned was where you began to think about having a longer period of detention. Was that from August 2004 onwards which was the start date for the investigation?

Deputy Assistant Commissioner Clarke: Yes.

Q261 Mr Clappison: So you started to think about it then. Were there working groups thinking about having a longer period of detention?

Deputy Assistant Commissioner Clarke: This was informal discussions with my senior colleagues about what sort of investigative strategies we were going to have to develop to deal with this sort of case. The informal working group thing about it was I sat down with a group of professionals and said, "What do you think? How can we get into this?" Interestingly, *** was the case which was referred to by Mr Owen in his evidence before this Committee where he was talking about custody time limits being loaded in favour of the prosecution and he referred to the fact that this case was due to start trial in April this year. I suppose, slightly ironically, the defence a couple of weeks ago put in an application to have it taken out and it is now actually listed for the autumn of this year, a lot more than two years since the moment of arrest, and the grounds of the defence application were that they have not had time to consider the weight of the material!

Q262 Mr Clappison: It has always been a part of your case that you wanted to stop developments early because of the threat to public safety from this type of offence really.

Deputy Assistant Commissioner Clarke: Yes, exactly.

Q263 Mr Clappison: You mentioned in ***, public nuisance through irradiation. That sounded rather alarming.

Deputy Assistant Commissioner Clarke: Well, this is a quirk of the British legal system. This will be addressed actually by the Acts Preparatory to Terrorism Measure. *** Because, under the current conspiracy laws, it is very difficult in these cases, where you are drawing material from a range of computers and other places, to actually prove the act of conspiracy, the agreement, what we have to revert to is a piece of 19th Century common law around conspiracy to cause a public nuisance which is quaint.

Q264 Mr Clappison: Yes, it did ring a bell and it sounded strange.

Deputy Assistant Commissioner Clarke: Well, in the same way as in Springbourne, Kamel Bourgass was convicted of conspiring to cause a public nuisance when what he wanted to do was basically to poison the public. Again it is about shoe-horning 21st Century terrorism into 19th Century common law which gives us difficulty.

Assistant Commissioner Hayman: Also, making this point for the sympathy vote, it must not be overlooked, and Peter actually described it, when you are trying to get your case together within the 14 days, the impact on our people is horrendous. Peter has described people sleeping on office floors and they are doing that. As for the people who are looking at CCTV footage, I saw one colleague go home and he had lost the whites of his eyes, they were completely bloodshot from where he was continually watching TV screens. Now, that is not a way of managing people in your investigations because you have to pull all the stops out to get within those timescales and the consequence of not doing that is heaven knows.

Q265 Chairman: You have obviously presented a case here that these are very complex cases and may involve very dangerous people, but, if we go back over the argument we have had earlier today and if we take *** and the other cases, the strength of your case for having an extended period is that you have to intervene early because these are cases where you need to get in early to protect the public as well as carry out the investigation. Can you point to any cases here where in practice you did that and people were very close to actually committing a terrorist offence? The alternative point of view to your case is that this may well be the case, but if you had carried on with another couple of months of surveillance or whatever, then you may have been able to extract more evidence prior to arrest while not putting the public at any particular increased danger of the attack being carried out.

Deputy Assistant Commissioner Clarke: I could point to the converse of ***, as it were, where we were able to manage the terrorist cell through control measures, through surveillance and technical intervention, *** We were able to mount a surveillance operation *** and it was probably the most extensive operation we have ever conducted in this country, enormous both physical and technical surveillance, so that gave us the comfort that we were fairly sure that they would not be able to mount an attack while they were under that level of surveillance. *** we were able, to use the jargon, to run it long until the point where we were able to say that, when we intervened, we would have unequivocal evidence of terrorism so that they could then be charged. *** I thought that it was absolutely critical for community confidence, because we had had a lot of criticism about arresting and then releasing under the Terrorism Act with no charges, that, if we are going to arrest a group of young British men on such serious allegations, we should be able to have unequivocal evidence to put before the court. Now, of course there is a frustration that,

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

in the public debate for the last two years, none of this has been able to be rolled out and I do sense that the public, for all the obvious reasons, are being denied a part of the information which would be so important to them and enable them to come to judgments. It is very difficult for us, particularly when we are speaking with the Muslim community, to explain the reality and the strength and the depth of the threat when we cannot actually allude to the sort of things which are currently waiting to come before the courts.

Assistant Commissioner Hayman: I am just thinking out loud here, but I think there have been three thwarted attacks since July. *** was one and I think there are two where discussions were being held as part of the investigation and the meeting that Peter chairs which is looking at the best time and the right time to predict where, and I do not want to put words into your mouth, Peter, but I know we had discussions that public safety is the predominant consideration here, decisions made to interject, and then what you think you are going to find actually presents you with more of a challenge to gather the evidence and it is whether you have struck too early and you really do not think you can balance or you can gamble with the public safety. I can remember one particular case where Peter and his team had been working like billy-o to get that within those 14 days, and I just think that you cannot help but wonder at times that, because you are working at such a rate of knots, the thoroughness may not be there always or it may produce hastiness, and, okay, you can repair that when you start to prepare the case for presentation in court, but that just seems to me to be a crazy way of operating.

Q266 Chairman: Going back to Springbourne, it has been widely suggested that it was a bit of a fiasco actually, that there was not any ricin, and that large numbers of people were found not guilty. It is one of the cases that is used to discredit the anti-terrorist operation. The police seem to suggest that this was one of the cases where further investigation would have led to more successful charges. Is that right, in your view, and obviously we do not know legally what the position is, but in your view?

Deputy Assistant Commissioner Clarke: I think with Springbourne there could have been a different outcome. Mohammed Meguerba was the individual who was arrested early in this operation, and, remember, this was a rolling operation from the spring of 2002 right the way through to the finding of ricin by-products in January 2003, the murder of Stephen Oake in January 2003 and the search of the Finsbury Park mosque in that same month. Meguerba was the man who was arrested in September 2002 and there was no evidence to charge him at that time in respect of terrorist offences. There were some issues around identity fraud and the like. He was released, jumped bail and went to Algeria and then it was in the subsequent three-month period that his fingerprints then appeared on a ricin recipe which had been recovered in Norfolk. Had he still been with us, he would have been

charged as a main conspirator along with Bourgas and the others. The broader issues around Springbourne are very interesting in terms of the legal process and case management, and the challenge which I think our criminal justice system faces in dealing with this new type of case where we have international conspiracies, information and intelligence coming from different jurisdictions and the, I hesitate to use the expression, the “game”, but I heard an eminent QC use it recently, saying that the “game has changed and we’ve moved on from the Queensbury Rules of the IRA”, he said, “to the new game which is to try and hit the PII bullseye in court”, in other words, test the information which is coming forward or try and probe to the point where the prosecution are obliged to relinquish or throw out the case because it would cause such jeopardy to international relations were we to proceed, and that is a new form of tactic which we are seeing evolve now. I do not know how that will play out during the coming year; we will see how our criminal justice system is equipped to deal with it.

Q267 Chairman: Taking that case as relevant to today’s discussion, it does not sound as though, had you had detention of up to 90 days, you would have necessarily got any more detentions.

Deputy Assistant Commissioner Clarke: Not necessarily on that, no, but I cannot say yes or no. I have been asked this question many times: “Tell me how many terrorists you have had to let go because you have not had 14 days, 28 days or 90 days”. As I said earlier, I think, with respect, that is the wrong question.

Mr Winnick: There is no contradiction between what you are trying to do and what we are doing to try and prevent this country from being the subject of terrorism and at the same time not affronting what may appear to be the long tradition in this country of the rule of law for protecting civil liberties. Mr Malik said that he respected your integrity and that goes for all of us, though differences may occur, and we have the highest respect for the work you do day in and day out—

Mr Malik: I said we all respected it, not just me.

Q268 Mr Winnick: We say so publicly, we have said so and we know the responsibility that you carry, but there are one or two questions. As far as the atrocities of 7 July are concerned, and there is no doubt that if there had been 90 days, 180 days or whatever, it would not have made the slightest difference, it took the police and security authorities totally by surprise presumably?

Assistant Commissioner Hayman: I am not sure what the question there is. What we are saying is that obviously the main perpetrators lost their lives, so, if that is what you are saying, the days would not have really mattered.

Q269 Mr Winnick: There was no suspicion about them, that is what I am saying, otherwise obviously they would have been brought in in the usual way. It is not a trick question. What I am saying is that this

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

atrocities which occurred and took the lives of 56 people on 7 July, it would not have made any difference if there had been 28 days or 90 days or whatever.

Deputy Assistant Commissioner Clarke: I have to be immensely careful in answering this because of the position we are at and because I do not want to mislead the Committee, but *** What I am saying is that I cannot say that 90 days would definitely have stopped 7 July, but neither can I exclude it as a possibility, however remote. ***

Q270 Mr Winnick: But you will accept, Mr Clarke, that, if that was the argument for 90 days, then, as Mr Browne and myself said earlier on, that could equally be an argument for longer because you could say, "Well, if we just had longer than 90 days, if Parliament had given 90 days, we might have found this or the other". The danger perhaps from the point of view of parliamentarians who took a particular view and voted accordingly on 5 November is the danger of escalation where you actually say in effect, "We stop here and no further".

Assistant Commissioner Hayman: I have just a slight concern that I would like to share. Regardless of the pros and cons of whether it is 90 days or not, what I think we are starting to paint here is a picture which is getting worse, getting more complex. With the technology that is starting to advance, it is a fair opinion, I think you could say, that in the next two or three years it can only get more complex and more difficult. I am just worried that the consequence of the debate we have had both in Parliament and in the public domain creates a difficult environment where, because of the things we are now starting to see, we need to go back in two or three years' time to review our position on levels of detention, and that this whole process and what went on in the autumn starts to make it so difficult to have that debate when actually we should be having the debate, given how the picture starts to unfold, and that is a concern I really have got.

Q271 Mr Malik: I understand where David is coming from. I think there has got to be a clear distinction, has there not, between pre-7/7 and post-7/7? The argument really does not seem to make too much sense to me if you are saying that, if you had been able to hold people for 90 days before 7/7, would 7/7 have taken place? Is it not the case that 7/7 has woken up everybody and it changes entirely how the Security Service and the police work and, if that situation arose again, then you would be looking at it in a different way? You would be operating in a different way with a different set of circumstances, so I am just a bit confused about the kind of circular debate we are having about the 90 days as that is just one aspect of the police and Security Service's work and there are many other aspects that have changed as a result.

Assistant Commissioner Hayman: Yes, I agree. If you took a snapshot pre- and post-July, I do not think you would see it radically different in the way we are operating because we have enjoyed

tremendous partnership arrangements without confusing the boundaries between unique roles. I think investigative capability and techniques remain the same, but what I would shine the light on where there is a wake-up call is around the community relations and embracing the community. I think that has been a big wake-up call for everyone and, if we look at the things we are planning now, that is radically different from what it was post- and pre-July.

Q272 Gwyn Prosser: In the public session, you made some cautious remarks about the way certain firms of lawyers and solicitors act on behalf of their clients and share cases. Do you want to expand on that?

Deputy Assistant Commissioner Clarke: I fear my remarks probably were not cautious enough. It is not for me to second-guess a professional judgment of lawyers because we do see certain patterns and I do find it strange when, say, we have nine people in custody, eight of whom are represented by the same firm, and they all receive identical advice even though their circumstances are radically different as I am not sure that each individual suspect is getting the best possible advice. Now, I can only speculate as to whether that might be because there is a wish to protect a leading party within a conspiracy from a revelation by other members of that conspiracy. I can only speculate on that and it would be improper for me to go any further, but nevertheless I sometimes feel that not everybody is benefiting from the most objective and professional advice.

Q273 Mr Benyon: You said earlier that you were content with the resources you had at your disposal. We had a meeting with Head of the Security Service, Eliza Manningham-Buller, last year and she said that the Prime Minister talked about there being hundreds of people who were causing concern, but that figure has since gone up to nearly 2,000, and maybe beyond. One got an impression that resources would never be enough really to be able to play it, but, in terms of this inquiry and your description of seeing one of your officers with his bloodshot eyes, you will never have enough resources really to be able to expedite an inquiry as quickly as you want, so can you go a bit further than what you were saying earlier in terms of answering Mr Clappison?

Assistant Commissioner Hayman: I am making those comments, I guess, as a bit of a realist really. Terrorism is a dreadful crime, but it is not the only crime and, when there is a limited amount of resources which need to be spread across a very broad agenda which is not just in terms of the Police Service, but right across the public sector, I just do not think it is right that you go in there trying to take the lion's share of the resources when actually the reality is that you are still going to be prioritising as you are now. That is where the professional judgment comes in to make sure that you get that prioritisation right because it is not a bottomless pit, and we all know that, so why go to the negotiating table being so bullish that actually you disadvantage

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

other important parts of the public sector funding, knowing in the back of your mind that you are never going to be able to meet the exact demand that you know exists? Therefore, I would rather have a modest settlement where I can look ministers in the eye and say that I will deliver on what I have promised I will deliver. Yes, it is not easy to keep prioritising. When I go to the briefings with ministers, I say to them, which is fact, "What is getting prioritised out at the moment post-July would, pre-July, have been a top priority". Now, that could sound horrific, but actually we are making those judgments on the basis that there are not enough resources to go around.

Q274 Mr Browne: It does not really need to be said in this session, but you were just talking about different types of crime and one of the other cases being made at the moment for amalgamations of police forces is to deal with terrorism and large-scale organised crime. I am just curious to know, as you are here, whether you think that will assist the process, whether it becomes more difficult and more fiddly, if you like, just having 43 forces in England where, I suspect, there is not that much terrorism concentrated in quite a lot of those forces, whether you think the process of amalgamation would help streamline your investigations or whether it would not actually help that much in that.

Assistant Commissioner Hayman: Well, I would put my cards on the table and say I am a strong advocate of fewer forces. I have worked in a smaller force alongside two other smaller forces and the extent to which I, as the chief there, could meet some of the demands not just of terrorism, but of serious crime, it was just impossible. We had the guy who had his fingerprints on the ricin menu in Thetford and, therefore, it meant that there was absolutely no way we could deal with that and we had to bow to the expertise at the centre and to the Met, so, for me, the configuration for something like this where you have fewer forces where collaboration and strategic position are at the heart of the way in which you order yourself, you recognise that, coming from London, there is a very specialist unit which is able to help and assist, but it is coralling what also is available around the rest of the country. I think there is the other piece at the moment which needs to be re-ordered which is part of the agenda for the next 12 to 18 months nationally and that is to get the gearing right in terms of terrorist investigations between intelligence-gathering and investigation and what we call "protective security", which are the things where you try to deter acts of terrorism. If we get that balance right and we have got it ordered in a strategic sense with fewer forces, I think that would be an awesome force to deal with not just terrorism, but also serious crime.

Q275 Mr Malik: One of my concerns is community relations and how well equipped the Met is by and large. They have got their kind of capacity and skills and some of the expertise and experience now in dealing with some of those issues, whether it is

intelligence-gathering or whether it is community confidence-building, but I am not confident at all that the majority of the constabularies around the country are anywhere near the Met and that leaves a real deficiency in terms of dealing with intelligence and other issues. How are we going to build up some of that network and structure across the country?

Assistant Commissioner Hayman: I am going to speak candidly now and say that I do not share your perception of what is going on in London, to be honest. I think there is still a lot of room for improvement. It is on the right track, it has got the right ideas, but it has not got the kind of depth of contact and the confidence that is required; there is a long way to go. If your judgment is that we are okay—

Q276 Mr Malik: My judgment is that, relative to other constabularies, you are a long way ahead, though I still say you have a long way to go, but that is a great concern that they are so far behind.

Assistant Commissioner Hayman: I agree with you there. It is not just about necessarily terrorism investigations or relationships with the Muslim community, but that can spread right across the crime agenda into drugs and serious crime.

Q277 Steve McCabe: This is a very simple question I wanted to try and ask. Obviously the whole debate about the maximum 90 days attracted enormous publicity and some people thought it was a great parliamentary event and others were not quite so sure and you said yourself that it may have made it difficult to discuss some of this. I presume that the purpose of producing this paper is to say to us that there were a lot of very serious cases going on and still going on and there is a more persuasive case than parliamentarians may have thought at the time. Are you hampered by the way we behave? Is there another mechanism by which you could communicate to parliamentarians which would maybe take this out of the newspapers and out of the parliamentary ether and allow that exchange which is really important to take place?

Assistant Commissioner Hayman: Well, we are up against the problem of sharing this material and we cannot get over that and we all understand that. I would not in any way want to obstruct what I think is a healthy democracy where we are having the debates in open because that could get misunderstood, albeit there is a daily contact which we have with both peers and members. I think it boils down to responsible reporting and that is where the effort and the lobbying needs to occur or it gets out of control. Who would have predicted the amount of publicity and the commentary that occurred around that awesome summertime? Maybe if we had anticipated that, we would have dealt with it in a different way, but I felt that we were acting responsibly and professionally and, as ever, if there is a quiet news day, maybe that contributes to it.

**28 February 2006 Assistant Commissioner Andy Hayman QPM and
Deputy Assistant Commissioner Peter Clarke CVO OBE QPM**

Q278 Chairman: I want, if I can, to pursue this because looking at the cases you have put in front of us, you can see that Parliament has left it at 28 days, which was Mr Winnick's amendment, and you can certainly see from these cases, I think, although we have not gone through it in great detail, how 14 days was up against the wire in terms of at least half of these cases. It is quite difficult at this stage to look at this information and sense that 28 days, which is a doubling of that period of time, would not make a very significant difference to what you faced in these cases. It is more difficult to look at these cases and to see where the argument that it must be more than 28 days comes from. Rather than argue it in general terms, and I know it is repeating a question to Mr Clarke about how many terrorists did you let go last week, but can you look at the cases here and highlight ones or aspects of them that lead you to believe that significantly more than 28 days would in practice be needed in order to be as effective as you want to be?

Assistant Commissioner Hayman: This discussion is such a difficult discussion because there is a bit of me which is saying, as we were when we were debating the technology, that the pattern which is starting to emerge means that we can, I think, quite reasonably anticipate in two years' time, 18 months' time or next week, I do not know, but we will come across a case which has live operations going on at the moment and one particular operation is exhausting our resources and the point of interdiction is being weighed up by Peter on a twice- or thrice-weekly basis. We are saying, maybe not analysing where we are now, that it is the pattern which is starting to emerge and only time will tell on that. Do you not think I have pored over this every week since this debate has gone on, changing my own conscience, changing my own assessment and judgment, and we fell on one particular timescale which, I think, got misconstrued or misreported really, skewed in the reporting. It was about the extension, not the 90 days, and that, I think, is the point and it is very difficult for Peter and I to answer that question against a benchmark of 28 days.

Q279 Chairman: Lord Carlile told us that there was a case simply put to him that there were cases where up to 90 days might be justified. Are you able to identify for us whether you believe that is one of these cases or a separate case? If so, what would it have been that led to that?

Assistant Commissioner Hayman: It is a separate case.

Deputy Assistant Commissioner Clarke: It is a separate case and, because it is in a slightly different jurisdiction, with respect to any Scottish members here, slightly different rules apply anyway. His briefing from the senior investigators in that case

was clearly that it would have helped. I am not privy actually to those details in that specific case. It was an offshoot of a case which was based in and around London, but it was dealt with entirely within Scottish jurisdiction, so I am not in a position really to comment in detail on it or the briefing Lord Carlile received.

Q280 Mr Winnick: There has been a more recent vote obviously, as you know, in the Lords which rejected not 90 days, but 60 days, and the Government, because of what the Home Secretary had said earlier, did not vote and, if they had voted in the Lords, it would have been five, 10 or at the most 20 extra votes, probably less, but there would have been a majority against 60. When the question of seven to 14 days came before the House, I do not believe there was a vote on it, but I do not recall anyone voting against, so there was no controversy. We recognised in the House of Commons at the time when Beverley Hughes put the argument that there should be an increase and in fact it was 20 May 2003. I am just wondering, would it not be wise to see how the 28 days goes, not that you have got much option, I accept that, and, if you really believe that there is the strongest case that could be put to Parliament in due course, then it would seem appropriate to do so? I find it difficult to believe that parliamentarians, if they were faced with a very, very strong degree of evidence, be it on the Government side or the Opposition side, would say, "No, no, we have agreed to 28 days", whenever it was, last year or three years ago, "and we won't consider any increase". In answer to the Chair, you said you could not point to anywhere here where more than 28 days was necessary, so I would have thought that would be the best way to proceed.

Assistant Commissioner Hayman: I guess some of the points of reflection on all of this can be summarised like this really: let us not lose sight of the position the Government found themselves in in the wake of an attack in July. Speed was of the essence, was my reading of that, and, therefore, maybe in the essence of speed in getting some legislation framed, some of the processes you would normally go through got compromised, and that is for others to make a judgment about. This process here seems to me to be very thorough and very strong in its scrutiny and, if you were looking for any kind of evidence-based development of proposals, it could come from some kind of scrutiny committee cross-party or something like this. I know that Lord Carlile, when he gave his evidence, certainly was an advocate of that and we would want to be a contributor. Of course that is with the luxury of time and I do not think that was there in the summer.

Chairman: Can I thank you both very, very much. You will want these papers back, I am sure, so we will return these to you.

Tuesday 21 March 2006

Members present:

Mr John Denham, in the Chair

Mr Jeremy Browne
Colin Burgon
Mr James Clappison
Mrs Ann Cryer
Mrs Janet Dean
Steve McCabe

Mr Shahid Malik
Gwyn Prosser
Mr Richard Spring
Mr Gary Streeter
Mr David Winnick

Witness: **Rt Hon Charles Clarke**, a Member of the House, Secretary of State for the Home Department, gave evidence.

Q281 Chairman: Home Secretary, could I thank you very much indeed for coming to give evidence this morning. As you know, this is the final evidence session of the Committee's inquiry into terrorism detention powers. We have taken evidence from a wide range of different organisations with different perspectives about this, and we very much look forward to your contribution this morning. Can I start by asking you, Home Secretary, about the process by which the Government came to support 90 days? It looks to be a very rapid process from the initial suggestion of the idea to the Government saying, "Yes, we support the police"?

Mr Clarke: Only rapid in the context of a "Royal Commission generated change". We did accelerate the timetable for the proposed terrorism legislation. If you recall, during the Prevention of Terrorism Bill 2005 and the debates in the House I committed to further terrorism legislation to implement some of the proposals about new laws and so on which, at that stage, we had envisaged happening much later than in fact took place. The change took place because of 7/7 and, following consultation with the opposition parties and others, we decided to bring forward proposals for new legislation when the House came back in the autumn, so that accelerated the process. In that sense I would say, yes, it was quicker than normal; but I do not think that it was unduly quick. We had a lot of discussion both across government and with a wide range of agencies and also opposition parties from the end of July and beginning of August through to mid to late September and the proposals about detention were in those discussions from the outset.

Q282 Chairman: Yes, but if I have got the process right the Government asked ACPO if it wanted any further powers and in response to that ACPO suggested a number of things, including 90 days, is that right?

Mr Clarke: Almost right. What we did was we asked generally, including ACPO, whether there were further powers that would enhance our ability to combat terrorism. ACPO came up with a number of suggestions, as you say, including the 90 days which we talked about. I then said, "Let's look at these things and see what substance there is and whether this is in fact necessary or not". There was a process that went on over the summer of looking at that.

Q283 Chairman: You say "over the summer" but in fact the proposal for 90 days was backed by the Prime Minister only two or three weeks after you had received it from ACPO?

Mr Clarke: Backed in principle. What was being said by the Prime Minister, and by myself, was that there was a whole set of proposals here for changes which were either necessary or should be considered and we, in principle, backed the need to look at them; but of course then we went back to the detail of "Do we need this?" and "Do we need that?"; and that was where we asked the police for their advice.

Q284 Chairman: When the Prime Minister said in August that "we backed the proposals for 90-days detention", he was not saying the Government had decided to back the proposal for 90-days detention; he just said then that in principle you supported it and were going to look at it?

Mr Clarke: Basically, yes. What we decided was that we backed not just the 90-day proposal but a whole set of different issues at that point and then asked in some cases Home Office officials, in terms of drafting legislation, and in other cases the police and security services for advice with a view to coming to proposals which I said at that time I would discuss with opposition parties and others from early September onwards, based on a more substantive examination of the case that was there. That was in fact precisely what happened. We went through the proposals with the benefit of that further assessment and came to the views for proposed legislation which we did.

Q285 Chairman: I have to say, Home Secretary, that sounds a little more tentative than I got the impression at the time. Do you think I am alone in thinking the Prime Minister had made a firmer commitment to 90 days in the middle of August than in fact you are now suggesting to us?

Mr Clarke: One of the disadvantages of my life is that I am not inside your brain, so I do not know exactly how you are seeing it! What the Prime Minister was saying in the strongest possible terms was that he was keen that the Government should give the legal support that was necessary to our police and security services to deal with the terrorist threat. Having heard this as a possibility he was very keen to say that we would want to be doing that if

21 March 2006 Rt Hon Charles Clarke MP

we could, having analysed it; that is what he said; and we went through the process then of going through it. If you look even at the famous 12 points that were at the end of that first week in August, that was a set of proposals some of which were subject to legislation and went through Parliament, as you know, and that was always the context in which it was. What he was saying was, "This is where we ought to be going, but of course we have then got to look at the detail".

Q286 Chairman: We have established, Home Secretary, that at the time the Prime Minister announced his support for 90 days the only written material supplied to the Home Office were three ACPO press releases and two sides of A4 describing two operations. Do you think, given the controversy that then followed, that was sufficient information on which the Government should base such a far-reaching decision?

Mr Clarke: The decision was the publication of the first draft of the bill in September. It was that decision which set out what the Government intended to do, including the 90-day clause. The Prime Minister's statement, indeed my statement in August, indicated where we thought we should be. As I said a second ago, what we then did was go to look in detail at the particular suggestions there were and come up with particular propositions that found their way into the bill. If it were indeed the case that a bill was to be published entirely on the basis of a press release I do not think that is a very good idea. If, on the other hand, the bill is to be published on the basis of seeking police advice on the best way to deal with the terrorist threat, which is what I think actually happened, I think that is a perfectly sound way of looking at it.

Q287 Chairman: The only further information that we are aware of that was produced by the police, certainly in written form, during the whole of this process, including after publication of the bill, was the letter from Andy Hayman which was circulated to MPs. What other information did you as Home Secretary request in support of the 90-day case before you reached your decision to support it?

Mr Clarke: I requested of all the agencies (and I will talk about them separately if you wish me to do so) their considered view as to what would be the most effective means of helping them to contest the terrorist threat in terms of people whom we suspected might have terrorist intentions but we could not prove that an act had actually happened. That was what I requested of Sir Ian Blair, Andy Hayman and of the police generally. They communicated their view that 90 days was the right way. We then got into—and I do not want to be misunderstood as I was going to say a "theological debate" but it is not quite right—a complicated discussion about, was it 90, was it 100, was it 80, and then coming down to 28 as we did. On each of those questions you were resting on judgments; you were not resting on actuality because it was not something, by definition, we had had experience of. It was also something where evidence from the

criminal justice system was not particularly appropriate because our criminal justice system is unique and rightly so. You were at a series of judgments and you had to decide whose judgment one valued in this; and I valued the judgment of the senior police.

Q288 Chairman: To what extent did you rest your decision on the conclusions the police reached, i.e. the conclusion that 90 days was the right figure? To what extent did you say to your Home Officials, "Can you analyse the case the police are making? Are they right about what they are saying about the disruption caused by the need for interpretation? Are they right about the problems of multiple representations by individual solicitors? Are they right about all of these—computer decoding and so?" To what extent did you ask your Home Office officials to independently analyse the police case? To what extent did you simply rest on what the police were advising you were their conclusions?

Mr Clarke: It is a good question but a hard one to answer. I think if I was to be frank I would say I rested quite a lot on the conclusion of the police case; but when you ask me, as we go down the different elements, about say the interpretation, encryption issues and the interaction of foreign international agencies and so on, if you look at each of those issues I did discuss each of those both with the police and with Home Office colleagues to satisfy myself that what was being talked about was a reasonable description of the state of affairs. You have used the word "analysis" and that was where I was struggling a bit in answering your question, because the extent to which it was possible to analyse each of those aspects in a very scientific way I think was quite limited and, by the way, is today in my opinion. I do not think there is an objective analysis which says, "The exact time you need for a particular case is X".

Q289 Chairman: What you have just said, Home Secretary, really matches what Assistant Commissioner Hayman told this Committee when he agreed with the following wording when it was put to him: "The question of whether the maximum period should be 90 days is much more a sense of instinctive judgment about what feels about right. Is that fair?" He said: "That is absolutely fair". The problem, Home Secretary, is that when you were commenting at the time of parliamentary discussions you said, for example, to the Joint Committee on Home Rights, "The Government found the case compelling for 90 days". Do you now regret backing 90 days and the Government backing 90 days so firmly when it is now clear that what the police were really say was, "Look this feels about right but we can't be sure?"

Mr Clarke: I think that is an exaggeration in both directions, if I may say so, with respect, Chairman. Yes, I do feel confident about what I have said and I think it was the right thing to do. Let me take both the other way round. The police make a judgment, and that is what Andy Hayman was saying in his evidence to you, which you have just cited back to me. They make a judgment; it is not a hunch; it is not

21 March 2006 Rt Hon Charles Clarke MP

a figure plucked out of the air; but it is an assessment, in their professional view, of what is the right thing to do. When pressed on that point—can 90, as opposed to 89, be stacked up—it is very difficult to do so. If you say 90 as opposed to 28, however, in contrast it is much easier to say 90 is a better time in terms of policing than 28 from the point of view of dealing with the terrorist threat that we face. I think that is what Andy Hayman was saying in the wording you have just described. You then ask why I use the word “compelling”. The reason why I use the word compelling is because the police advice is compelling; and because the narrative which they give, which is set out in Andy Hayman’s letter, is even more compelling. If you talk, as I have done, to those who professionally are responsible for de-encryption, for example, you find it is something which is very difficult and takes a very long period of time. At one level, who cares; but at another level, if you are talking about the liberty of somebody who might be able to blow up a tube train, it is extremely important. I saw each of those arguments, which you have just outlined, as of themselves a compelling narrative to make the case for a longer period of detention; always bearing in mind of course that that longer period of detention was subject to judicial overview in a very tight way throughout the whole of that process.

Q290 Chairman: Finally, Home Secretary, in early August we had a cross-party consensus in response to the London bombings largely (not entirely) as a result of this individual issue. The cross-party consensus broke down; you failed to achieve 90 days and you have ended up with a position which you are not now apparently going to change (and we will come to that later); you have ended up with a position which is much less than is necessary for the security of this country. In retrospect would it not have been better, for example, to put such a controversial decision in front of a select committee like this one to scrutinise the issue properly, to air the debate in a more constructive way, than happened in the House with all sides, and to then come to a conclusion? Would you not actually be further forward if you had done that rather than taking the approach that was taken?

Mr Clarke: I do not think so. I always agree it is best to put things in front of a select committee for scrutiny in terms of pre-legislative scrutiny or whatever process you have available, but the fact was the time was not available in these circumstances because of the events of 7/7 and the need to legislate, in my opinion, rapidly. Let us recall, the events of 7/7 took place on 7 July and we are now here on 21 March and we still do not have legislation on the statute book, and the time our process takes is very substantial. I do not know if you have taken evidence from the opposition leaders on this but I think the integrity of their commitments to looking at the 90-day process was very clear from the outset, that they had questions to ask. They never committed and said, “We think 90 days is the right way to go”, but I came to the view at the end (and I do not know if you are going to pursue this)

that actually they were not ready to discuss anything certainly beyond 28 but even less than that; and they simply were not able to act in any way. The choice I faced was, knowing that was the case, did I proceed with seeking to get agreement on 90 days, which is what I did, which was the police advice I had; or say that is just not on because people, for what seemed to me wrong reasons, were opposing it?

Q291 Mr Winnick: I believe, Home Secretary, that when it was increased from seven to 14 days there was no division in the House?

Mr Clarke: I do not have the figures in front of me but I certainly do not contest that.

Q292 Mr Winnick: So we have a united House of Commons. What unites us, does it not, Home Secretary, is the recognition (indeed before the horrors of 7 July last year) that this country is indeed faced with acute danger of terrorism; and no-one as far as I know in the House of Commons disputes that in any way, and even before 7 July? Do you accept, Home Secretary, that if the period of detention had been longer, or shorter for that matter, it would not have made any difference to the horrors which occurred when some 56 people were massacred on 7 July?

Mr Clarke: I have two observations about that, Mr Winnick. The first is: I do agree with you that the length of the period of detention would not have been a relevant factor as far as the 7 July events are concerned because they came out of blue skies.

Q293 Mr Winnick: I am sorry to interrupt you, but the period of detention would not have mattered in the slightest when it came to the massacre of 56 innocent people on 7 July?

Mr Clarke: I agree. Precisely so, because it was not that we had suspects who were about or a fallback event. It came out of a blue sky, so I agree. As it happens, I do not actually accept the proposition you made in the introduction, Mr Winnick, that everybody accepts the danger of a terrorist threat. I think they do now, having had 7 July. I was very struck in the debates on the Prevention of Terrorism Bill before the General Election because I think there were a number of people who simply did not believe it was real to talk about a terrorist threat. They might not have argued that and very few people will have been so foolish as to argue it as explicitly as I have just said, but I think there was, at a minimum, a very widespread scepticism across some parts of Parliament about the question of whether there was or was not a terrorist threat. There are suggestions that the Government was “talking it up” in a dishonest way before the Election for political reasons and it was a completely invented thing. I do not accept the prior point. After 7 July of course, by definition, people do accept there is a terrorist threat, although again now there is still scepticism about the extent to which that exists.

21 March 2006 Rt Hon Charles Clarke MP

Q294 Mr Winnick: I think you will agree, in all fairness, if there were any Member of the House of Commons who were disputing the terrorist threat before the General Election it certainly did not include me?

Mr Clarke: Of course I am not talking about you personally, Mr Winnick. Throughout all the time I have known you, you have been very, very clear about this threat. In the House there have been no parts of any of your interventions which have been informed by anything less than a determination to fight terrorism.

Q295 Mr Winnick: Then we agree on one point! You have an ally, Lord Carlisle who, unlike his party, argued in favour of 90 days. But when he gave evidence to us, not deviating from the view which he has consistently expressed, he did say there was a matter of trust, that perhaps because of what happened, say, three years ago, a matter concerning Iraq, people had less faith, be it Members of Parliament or the general public, over what the Government may say. Do you feel that he was right when he said that the Government's case to some extent was undermined over this question of trust?

Mr Clarke: Very much so. I very strongly think that. In particular I think that the whole story of weapons of mass destruction in Iraq led to a lack of confidence in the security services and intelligence assessments, which is very widespread. I argued that in public, both in the House and also in front of other select committees, not this one, but the Joint Committee on Human Rights, before the Election and subsequently. I think a central task of government is to regain the trust of the country in the integrity of our assessments of this kind. There is no doubt that the whole story of WMD undermined the confidence and, therefore, trust in the assessment of the Government in these matters; and that for me, as Home Secretary, has to be a central problem and issue.

Q296 Mr Winnick: On 26 October last year you told the House that you would try and reach a compromise. I made an intervention to see if consensus could be reached and I said it certainly could not be reached on the 90 days, and you said that you would continue to try and find some consensus: "...I am ready to be flexible in discussions, if we can reach an agreement." The impression was obviously that you would do your best to see if such an agreement could be reached without dividing the House; but you came back not with some other figure but you stuck to 90 days. Would it be fair to say that someone, in this particular case above your grade, insisted that 90 days must be the position?

Mr Clarke: Not at all, it would be entirely wrong and factually incorrect. I am grateful for the chance to set out exactly what happened because it was, as you say, an exchange with you personally across the floor of the House which has given rise to a lot of these situations. I stated to you and stated to the House that I was ready to be flexible to try and secure agreement. I had talked previously to opposition

leaders about this matter. I had not got a great sense of flexibility but some readiness to move perhaps. I went to see David Davis, the Conservative leader in the House on this on the Thursday afternoon after those exchanges and we had a one-to-one conversation in his office in the Commons. He was doing a debate that evening against the current leader of the Conservative Party in their leadership election which was taking place and he was off to do the Question Time debate, and I said, was there any possibility of him coming off the 14 days, and he said he could just conceivably imagine getting up towards 28 but, under no circumstances, going beyond that; he would certainly never be in a position to be able to recommend that. I asked him to reconsider. I said to him if he wanted to talk to me over the weekend would he please do so and call me because I needed to know whether there was any chance of flexibility from the Conservative front bench on that question. I thought there might be actually, because I thought in the Conservative leadership election in the interests of a country facing terrorism there might be some readiness to be flexible on this. I have a good relationship with David Davis; we talk quite frequently; we try to operate in the multi party way that the Chairman was describing a second ago; but he did not phone back over the weekend. I phoned Mark Oaten from the Liberal Democrats also on that Thursday and said I did not expect him to change, because the Lib Dems had been very clear throughout that they were not going to change at all, but if he did have any desire to change would he let me know over the weekend. Again, he did not come back to me. We then had the meeting that was pre-arranged on the Monday morning where Dominic Grieve was there for the Conservatives and Ms Featherstone was there for the Lib Dems—David Davis and Mark Oaten could not be there for various reasons—and I said in terms to them at that time, "Again I say to you, the group," (and the Scot Nats and Welsh Nats were also there), "is there any chance of flexibility above the 28 as far as you are concerned?" They said, "No, there is not. There will be no move on that as far as we are concerned". That was a big statement from my point of view because I had hoped there would be some flexibility on that matter and I thought it was important there should but, but they were very clear there was going to be no flexibility whatsoever. The suggestion afterwards by some speaking on their behalf that there was flexibility I believe was dishonest. I do not think there was an intention to be flexible at all in that area. I then looked at the question of flexibility and I talked as you know, Mr Winnick, with a number of our political colleagues on the Labour side to see what they felt about all this; and actually what had happened over the weekend as you might acknowledge (and I do not know if you would or not) was there was a strengthening view, because many had conducted polls in their own constituencies and things of this kind, that we should stick with the 90 days. I interpreted the best way of trying to get flexibility as to not come down with 90 days but to have 90 days plus the review clause as

21 March 2006 Rt Hon Charles Clarke MP

something you yourself had pressed in your approach. I thought 90 plus the review a year later might be a more flexible way of attacking this than reducing the number of days from 90 downwards, and that is why I have decided to press on with that. There were two big factors which changed the situation from the exchange we had across the floor to the position I put forward in the House. One was the absolute obdurate refusal of the Conservatives and Liberal Democrats to change above 28 whatsoever in any circumstances; and I should say no number was ever raised by them in any circumstances, of 60, 45 or whatever. Secondly, the strengthening feeling in our own side of the House that 90 days was what we should stick with having listened to the police advice. The flexibility for me was 90 plus the review, which I hoped would carry it through. I did discuss it with the Prime Minister certainly, as I think you would expect me to do; but the suggestion you are making that he somehow told me to go off the position that I said in the House when we had the exchanges on that day is simply wrong.

Q297 Mr Winnick: I see. Fortunately we do not legislate by opinion poll.

Mr Clarke: I do think, Mr Winnick, in that very debate I urged Members of Parliament of all parties to go back to their constituencies and talk to their constituents about these issues, and talk to their local police about what happened. I can tell you a large number of Members of Parliament did precisely that, and that affected their thinking about how to deal with the issue when we came to the legislation later. That was not an opinion poll-driven thing but there were some who had their own polls based in their own constituencies.

Q298 Mr Winnick: If I may say so, in 31 years of membership of the House of Commons I do not always accept the views of constituents; I hope in most cases I do; but I also make my own judgment.

Mr Clarke: You would listen to your constituents would you not, Mr Winnick, but you would not allow them to tell you what to do but you do want to hear what they say?

Q299 Mr Winnick: I think we have to make our own judgments and then constituents decide, in our democracy, at election time. Could I bring you up-to-date, Home Secretary? The Government states that it now accepts 28 days and since the vote in the Commons the House of Lords have rejected 60 days. If they rejected 60 days I think it is pretty obvious what they would have done if we, the elected chamber, had decided on 90 days. Be that as it may, the Government now accepts 28 days. There is no desire to change that, am I right?

Mr Clarke: I do not think that is entirely right, no. I accepted throughout the passage of this bill the decision on your amendment that was taken should last through the passage of this bill to carry it through, and I think that is the right position to adopt. I think it would have been wrong of us to seek to change the decisions of the Commons, for

example, in the Lords, even had it been possible to do so, or to seek to revisit that decision after it had gone in that way. I did not agree with the decision when it was taken by the House but I respected it and thought that was the right course to follow. When we come to the new terrorism legislation in 2008 or whenever we come to it (2007 I hope) we will need to look at all of this, including the definition of terrorism which Lord Carlisle will help us with which was a big issue of controversy in the House during the course of the passage of the bill. I do not think we should pre-judge and say that what we have got, for example, on the length of detention is there forever. In so doing (for the avoidance of doubt) I am not advertising a view that I wish to revisit the 90 days when we come back. I am not saying the opposite either. I am not saying we are simply accepting it will be 28 come what may. We need to see what has happened over the period in between as well.

Q300 Mr Winnick: There is quite a possibility, within the measure of consolidated Anti-Terrorism Bill before the House of Commons, the Government will seek to increase 28 days?

Mr Clarke: No, I am being very clear. I am saying I am not committing myself to saying we will back 28 come-what-may when that comes around; but I am also not advertising any view to seek to change that. I am saying that we should come to a view as to whether we should seek to change it when we get to that point; but I have not got some back-of-my-mind view that this or that is the way to deal with it. I am acutely aware of the view of the House, as already expressed, and believe that that needs to be taken very seriously.

Q301 Mr Winnick: One last question from me. Has the Government learnt anything from what happened on 9 November last year, except for a wish not to lose future votes?

Mr Clarke: Parliament has to make its decisions is what I think. I am very clear about you, Mr Winnick, and have been clear in the House and elsewhere about your integrity in dealing with these issues. Personally I think there is someone at the other side of the House who allowed party political considerations to go ahead of any consideration of national security and I think that was unfortunate.

Q302 Mr Streeter: Briefly and following on from the last question, Home Secretary, we all understand the difficult balancing act you have to make between civil liberties and security: you wanted 90 days; you have got 28 days. With the rich benefit of hindsight, if you could have your time over would you have done anything differently in presenting your arguments to the House of Commons? Have you learnt any lessons from the last six or nine months in getting the period you wanted?

Mr Clarke: It is a good question and a difficult question. I would say, going back to what the Chairman said earlier on, that there is benefit in scrutiny, for example, through a select committee of these issues, and that is why I think that is of benefit.

21 March 2006 Rt Hon Charles Clarke MP

I do not think we had that option seriously on the timescale that we were on, on this particular piece of legislation following 7/7, and that is my view. I think the only thing to say is that I have to be self-critical about my own powers for advocacy in that particular situation; but there we are—that is life. That is in the interplay of politics which is, at the end of the day, how Parliament comes to its view. People take their views with different decisions. I know, for example, there were a significant number of members of your side of the House who thought 90 days was right but felt they were whipped into a position to go the other way; just as I am sure there were people on the Labour side of the House who did not really feel happy about 90 days but felt they had to support the Government position in that way. I think that is just how we have to look at the issues. Maybe I should have been more articulate in what I had to say, but I do not regret going for the 90 days. I think that was the right thing to do and I still think it was the right thing for the country.

Q303 Mr Clappison: I have some sympathy for the position which the Government has put forward in this but I have to tell you that I cannot accept the point which you have just made earlier on about the way in which Members of Parliament approach this on any side as far as I am concerned. I think people have found it a very difficult decision. Can I ask you about what you have just said about the process which you are now following because you have told us you have got an open mind on this (I think that is a summary of what you have said) as we approach further possible terrorist legislation in 2007/2008? Is there any work going on in the background of this in the Home Office?

Mr Clarke: On the 90 days specifically?

Q304 Mr Clappison: On the length of detention, the 28 days?

Mr Clarke: The answer is yes. We have got background work going on at the moment as to how we would put forward a codified approach for counter-terrorism 2007, as I said to the House, and that is all aspects therefore including periods of detention in that area as well. There is not specific work going on on this, as opposed to the overall body of counterterrorism legislation.

Q305 Mr Clappison: Will you learn the lessons which have been outlined today about the way in which the process was conducted in this and present the case a different way?

Mr Clarke: For the avoidance of doubt, Mr Clappison, I know you personally took both a great interest in this issue in this position and the principles of addressing the issues and your own contributions to the debate. My general remarks about Parliament's consideration certainly do not apply to the way you were looking at it. I think the approach which I set out in a statement to the House earlier this year of trying to bring all the counterterrorism legislation we have, ideally including the Northern Ireland counterterrorism legislation, into one permanent legislative

framework does have a much more considered approach to all of it, including pre-legislative scrutiny and the ability to debate much more fully where we can get to. Whether that will at the end of the day get us to an all-party agreement on where we need to be is, I think, a very interesting question and I do not know the answer. It does not depend only on me; it depends on how opposition parties decide to address these matters as well.

Q306 Mr Malik: Good morning, Home Secretary. The police and you yourself have said that the nature of the terrorist threat has actually changed because of this phenomenon of suicide bombers. Indeed, I have said it myself as well in the past. The large majority of recent cases have not involved suicide bombers, so what exactly has changed?

Mr Clarke: There are a number of aspects of terrorism which have changed fundamentally. The first is the nature of the terrorist organisations. I think what is quite important is to distinguish between campaigns in the 20th century essentially for national liberation of a variety of other struggles in different areas, which had a clearly defined focus and clarity about what they were seeking to achieve even if there were methods used which you and I probably would find unacceptable. The al-Qaeda terrorist ideology cannot be described in that way. The 20th century struggles were essentially products of enlightenment. The al-Qaeda struggle is essentially an attempt to recreate a medieval form of society which is against every value for which progressives have fought for centuries in this world. Firstly, the origin of the terrorism is different. Secondly, its character has been international, and is of a quite different order from many of the terrorist issues which existed in the 20th century; and the nature is quite different. Thirdly, the wealth and sophistication of the terrorist organisations is, again, of a completely different order, and with large amounts of resource being spent in most sophisticated people and equipment to try and deal with the threats that they have and very high levels of organisation. 9/11 itself is a classic illustration of that fact. The final thing is something you mentioned, which is the question of people's readiness to kill themselves in committing these acts, which is again different from the terrorists' struggles of the 20th century in general in any part of the world that you look at. I am not saying there was not accidental death, but deliberate death takes you into a different situation and means that a different set of criteria start to come into play because you then need to start discussing what you do to prevent a terrorist act, rather than what you do to bring the committer of a terrorist act to justice and they are different questions.

Q307 Mr Malik: One or two questions on community relations with respect to pre-charge detention. Of those held for longer than seven days under the existing terrorism legislation about one in three was released without charge. Will not

21 March 2006 Rt Hon Charles Clarke MP

prolonged detention lead to a significant worsening of community relations, particularly if people are detained for a long time and then released?

Mr Clarke: It could do if there were not a very clear awareness of the situation, firstly, by the police themselves in the decisions they are taking—and I think most people would acknowledge that the police themselves are acutely aware of the community tension issues which you describe—but also if the courts were not aware of it—and the fact that there is a return to court to extend detention on a very, very regular basis under these proposals means that courts could consider these questions as was necessary in any agreed case. I can accept the principle of the idea that community tension could be raised by bad decisions about keeping somebody in detention but, firstly, I do not think there is any reason to believe there would be bad decisions about that, because both the police and the courts would be constantly having that very, very much in mind; and, secondly, I believe that if there were any evidence of community tension-raising as a result of that people would be very responsive to that. I think there is just one other point I need to make which is the discussion I have had with a number of organisations (including the Muslim Council of Britain) very directly: there is no identity between being a terrorist and being a Muslim, they are different things. Terrorism can come from a set of misplaced religious views of course, including Islamist views, but they are different things. The fact that somebody is suspected of being a terrorist is not an attack on the Muslim community and I think that is a very, very important distinction. There are some who try and confuse this from all kinds of stances, but I think it is very important to keep them separate throughout our considerations.

Q308 Mr Malik: Finally, Home Secretary, I had the misfortune to be the Member of Parliament in a constituency where the Leeds suicide bomber resided. It is a constituency which has the highest BNP vote in the country and the highest number of racial incidents reported in West Yorkshire. According to your statistics from the Home Office 11 people were held since the new laws came into being on 20 January 2004. Between then and September 2005 11 people were held for the pre-charge maximum 14 days and all 11 of those people were indeed charged. I have an Opinion piece here I just want to read to you: “872 innocent people have been locked up for 14 days and imagine if these people, mainly young men, had been locked up for 90 days, the equivalent of a six-month prison sentence and then just dumped back in the community. It’s enough to tip any “normal” young man into the realms of a radicalised fanatic”. That is something that has been published in a number of journals and newspapers. It is actually written by one of my constituents, a Mrs Sayeeda Hussain-Warsi who happens to be one of the vice-chairs of the Conservative Party. Assuming that the Home Office is correct about these 11 people and that she is indeed wrong, then does not information of this nature seriously undermine community cohesion,

undermine confidence in the police, create unnecessary anxiety, feed victimisation and alienation and is ultimately completely and utterly reckless and reprehensible?

Mr Clarke: It is the first time I have heard that particular piece, but what I do agree with very strongly, Mr Malik, is that disinformation is more damaging in this area than any other area of public life. It is, in my opinion, an obligation on all those who comment and give opinions from whatever political party, from whatever orientation, to talk about the facts in a considered way rather than by developing misrepresentations in any particular area. I believe that is an obligation on all of us in democratic politics and one that is particularly pressing at this time.

Q309 Mr Spring: Home Secretary, I will not ask you recall your own conversations—

Mr Clarke: I dream them actually!

Q310 Mr Spring: I think civil servants traditionally have been there to listen in and that has always been the practice. The point I wanted to lead onto is this whole question of intercept evidence because I think it was in October last year you indicated this matter was under review, but in the submission you gave us you talked about it not being a silver bullet. You talked about the fact that any changes to the law which you thought were actually the disbenefits outweighed the benefits. It is interesting to note that civil liberties organisations actually have in general no problem with this, and of course it is very widely spread as a practice in other parts of the world. I would just like to ask two questions, and one is a general one: given the fact that there is a lot of interest in this subject, and there has been a lot of argument about this, I am just curious to know why in coming to the conclusion you did you have done so rather quietly? Having promised a review, we have not heard much about your actual reasons in the public domain. The second question I just wanted to put to you as an adjunct to that, I wonder if you could confirm my understanding, which may be inaccurate, that we are actually, in cooperation with other intelligence services, happy to use intercept evidence which they have garnered as part of the information that we receive from these security agencies but we do not do it ourselves? I wonder if you could answer those two points.

Mr Clarke: Firstly, I have a standard response when anybody asks if any particular measure has stopped any particular act, which is to say there is no silver bullet which solves everything, and I believe that is the case. If there were a silver bullet we would all agree to it, it would all happen and we could stop all terrorism. The question is a balance of judgment whether, in general, particular measures would help or hinder. Secondly, I do not accept that I have behaved, on interception, in a quiet way. I have made statements to Parliament about it from early 2005 onwards where I have tried to set out as clearly as I can the Government thinking on these issues and it essentially comes down to three points. Firstly, we agree in principle that if we could have intercept as

21 March 2006 Rt Hon Charles Clarke MP

evidence available that would be helpful for law enforcement in a variety of different reasons; but, secondly, there are two problems we have not solved: the first problem we have not solved is how we make that available without making the defendants aware of the way in which we have collected that intelligence which could be damaging to our overall intelligence interests; and the second is how we deal with the issue of disclosure, and the fact that the defence would always say, if there was one particular intercept which was given in evidence, “Can we see the records of every other part of intercept that you have”, which means you have a massive, massive data collection issue around it in a particular way. Do we think these two problems are soluble? They may be, particularly as technology is changing so rapidly in this area. That is why I committed to the House to conduct the review we are having at the moment and to report by the end of this year, in the hope that we can get agreement on this. I perfectly understand, Mr Spring, and you are right to say that there are a lot of people who think this is the right way to go, and it has benefits in their cases and other regimes and other jurisdictions where it can work. The two problems I have given are real problems and not imagined problems. They are not quietly addressed. As I have said, I have said them to the House explicitly in terms on a number of occasions starting from early 2005 so they are not secret but they are real issues and we are working to try and solve them. On using other countries’ intercept, I am afraid I am not familiar with the detail. I do not want to be misleading in what I am saying and perhaps had better drop a note to the Committee about it.¹ My understanding is that you are right, but I do not want to confirm you are right without being absolutely clear on the legal position about intercept again by other people being used in our courts. If you will excuse me, I will write to you.

Q311 Mr Spring: Thank you for that answer, but I think it is our understanding and I do not want to pre-empt what you are going to say.

Mr Clarke: It is my understanding.

Q312 Mr Spring: If that is the case then I think it does obviously beg a question. On your point about the review, and I understand that you want to proceed and do this in a comprehensive way, although other countries, fully democratic countries, certainly have no problems with this, I simply point out that you have made this point several times, Home Secretary, about how anxious you are to listen to the police, and when the police indicate they have a desire for something you react. I would just mention to you that we have had ACPO in front of us and they have made it clear that as far as intercept evidence is concerned, they would like to move on. We did specifically say this.

Mr Clarke: I do know that, Mr Spring, but it is my political opponents who have put the charge that I unthinkingly do whatever the police say, not I. I argue that I have a duty as Home Secretary, and

Parliament has a duty, to listen to what the police say and take it seriously, which I do; but I do not say that simply because the police say something it is our job as Parliament to do it.

Q313 Mr Spring: We will be looking forward to your comments on the use of intercept evidence, and I am sure that will help inform your ultimate view. Could I just move on to one last aspect away from intercept evidence, which is the whole issue of interviewing suspects. I think it has been something of a revelation to members of the Committee about how the actual process of interviewing suspects is obviously a very important but very small part of the whole process of actually garnering evidence. Given the fact that this is the case, and we have taken comments from people like Lord Carlisle and the Deputy Assistant Commissioner Peter Clarke, is the point of extended detention to allow time for the police to gather other evidence? Given the fact that it does now seem clear—as far as interviewing is concerned, it appears for a variety of reasons to offer limited value in these investigations, is that the logic?

Mr Clarke: I think both Mr Hayman and Mr Clarke in evidence to you stated that the purpose was not simply to question but also to gather evidence in the way you have said, and that certainly is the case. That is why, when the Chairman asked me how it was that I found the position compelling, when you look at the gathering of evidence from encryption, or the gathering of evidence from what comes from overseas intelligence agencies, or the gathering of evidence from enormous forensic sweeps which take place, it does take time for that evidence to arrive. It is the collection of that evidence which becomes a further factor which can then inform further interrogation in those circumstances. It is not a sense of perpetual interrogation over X number of days; but a sense of holding somebody who can then be asked about new evidence that arises following the time it takes to gather that new evidence.

Q314 Chairman: Just to pursue that point. We have been told by a variety of sources that the vast majority of people are simply going to be advised not to say anything—a perfectly reasonable response under our system for a defence solicitor to say that; and therefore changes in the law about that implying some level of guilt have no effect on the court whatever so people are advised to say nothing. Even if you do find other forensic evidence the reality is that those in detention are not likely to speak, are they?

Mr Clarke: It depends what you find, does it not? If one finds forensic evidence that clearly links through DNA, for example, a particular individual to a particular scene of crime that is so explicit and so direct that I certainly do not assume that there would be no response if an individual was questioned. I know that the lawyers we are talking about always advise their clients to say nothing so committed are they to the spirit of justice; but the fact is I do not think we can assume that that will be what carries through on each occasion; it depends on the evidence which is gathered.

¹ Ev 102

21 March 2006 Rt Hon Charles Clarke MP

Q315 Chairman: You would not challenge the evidence we have had, including the police evidence, that certainly those they regard as leaders or directors of terrorism are very unlikely to answer questions in this way?

Mr Clarke: No, I would not challenge that evidence. The balance of your question is right. It is obviously the case that people are advised to keep absolutely silent and often do so. I am only saying they do not always do that but I am not seeking to challenge the overall balance of the evidence you have had from the police on this which is more informed than mine.

Q316 Mr Browne: Home Secretary, moving on to some of the alternatives to increased detention that have been mulled over by Parliament and elsewhere during this process: resources and money. You yourself have rejected this as a complete solution and have cited the police in particular saying that in the later stages of investigation the events are quite often sequential and, therefore, it is difficult to do several stages of the investigation simultaneously. Nonetheless there is still a body of opinion that believes that logically if you double the number of people searching through computers or any other form of evidence you are likely to reach the needle in the haystack quicker than if you have fewer people undertaking that task. Are you happy and confident that we have sufficient people and sufficient money being put into anti-terrorism that that is not an alternative to having extended periods of detention?

Mr Clarke: I am confident of that as you ask it. I would always say more resources could be helpful. I think this Government has allocated record resources because the needs are so great, and the Chancellor has been very positive on those matters. I would never say that we would not benefit from more resources—that is always the case; but the qualification you put in your question, i.e. the extent to which we reduce the need for detention, I agree with you, that that argument is not made. I think there are cases where more resources being thrown at a problem have helped to solve it quicker—the needle in a haystack model. It is also the case, as you also said in your question, that there is not a direct relationship between the amount of resource you put onto the task and the speed with which you crack it because there are sequential issues, as you rightly say, which mean you cannot just say putting more in solves the problem. I do not believe that producing infinite resources would lead to a state of affairs where the detention issues were not still necessary.

Q317 Mr Browne: Just as a supplementary to that, it is a personal question really, you told Parliament that, in order to protect the British public from terrorism, it was necessary to detain suspects for 90 days. We are now in a position where they are detained for less than a third of that period as a maximum, which would lead anybody to conclude that you are presiding over a system where the public is at greater risk than you would wish the public to be. There is an onus, is there not, on your department to look even more searchingly at

alternatives, given that there is this inbuilt risk in the legislation which you have been unable to prevent despite your best efforts?

Mr Clarke: Yes, but I think the onus is even more on those who voted against the proposal for 90 days to examine their consciences on the situation, since it was their decisions which led us to a state of affairs where we are less well protected than we should be. I feel happy with myself on that. Those who did not vote for the 90 days have to ask themselves if they are happy with that.

Q318 Mr Browne: But we are less well protected than we should be at the moment?

Mr Clarke: Yes, in my opinion, as I have argued throughout on the 90 days.

Q319 Mr Browne: The other subject I wish to briefly explore was raised by the then Home Affairs spokesman for my party, the Liberal Democrats, which was the possibility or the option of charging suspects with a lesser offence—the Al Capone strategy as I think it is going to be known by some. While you were gathering evidence, while the police were gathering evidence on the more substantial issues relating to terrorism this approach was rejected. Can you expand your thoughts on that, particularly now that Parliament has limited the period of detention to 28 days rather than 90?

Mr Clarke: Firstly, I think it is fundamentally dishonest. To try and detain somebody on the basis which is not the basis on which you are actually concerned about them is dishonest; and I think the Al Capone strategy of attacking serious and organised crime through the Inland Revenue is not necessarily the right way to do it. Secondly, I do not think it actually works, because if there are questions of people who are potentially committing terrorist offences or preparing to commit terrorist offences a lesser charge will not do. It is true that we are assisted by the new charges which are in this current bill, which gives us some possibilities where we may be able better to deal with that. You can abstract from the situation that you need to charge people with the charges which you are actually interested in, in these cases; because it may very well be that they are guilty of a particular charge but they are not guilty of anything else at all, so there is not another charge which is available. To hypothecate your whole strategy for dealing with terrorism on the basis there may be some other charge—benefit fraud or whatever it might happen to be—I think is a mistaken view. I think integrity in this whole process requires one to face up to the issue. That was an argument I made to Mark Oaten but he unfortunately did not agree.

Q320 Steve McCabe: Home Secretary, Lord Carlile said that the extent of the control order is “so great that they come to the very limit of restrictions on human rights”. If that is the case, would not control orders be an effective device on those suspected of serious offences?

21 March 2006 Rt Hon Charles Clarke MP

Mr Clarke: They could be, and they take you quite a long way forward, but the question still remains, when you look at the danger of individuals and the danger that they pose—going back to Mr Malik’s question in a context where that can include catastrophic action, including killing yourself as you do that—then the question we have to ask ourselves, and I certainly have to ask myself, is: is the regime tough enough to deal with the threat which is posed? Control orders are an effective means of operating but they are not detention. If I consider it necessary to go to detention, so-called non-derogated control orders, I would certainly put that to Parliament, and Parliament would have to decide upon it but I do not think we are in that situation as we speak. The orders themselves are a partial response to this problem and not a total response to the problem.

Q321 Steve McCabe: If that is the case, if we were to combine control orders plus tagging and other surveillance techniques with the existing pre-charge detention period, would you be confident that would allow you to disrupt terrorist activities?

Mr Clarke: It is the same answer really. I would be confident that it is better than not having it, but it is not as good as having the ability to detain someone for questioning based on the evidence that is acquired. This is a very high risk game. With control orders, with tagging and with surveillance there is always a question of how secure is that. People are reasonably going to say, “Is it as secure as putting somebody in a prison cell?” The answer is that it is not. If it is not as secure as putting somebody in a prison cell, what is the extent of the risk we are bearing if that arises? As Mr Clappison said in his introduction, it is right there is always the balance between individual liberty and security and I completely accept that, but I cannot ignore the risk factors which are involved in all of this. I think that some people, and certainly not you, Mr McCabe, try and evade the sharpness of the choice by saying, “Can we stack up a whole range of measures which are equivalent to giving us the security of putting somebody in a prison cell?” The answer to that is, “Well, you can’t”. At the end of the day all of these measures, like control orders and so on, are not as secure as putting somebody in prison. Then of course the question arises, how can you put somebody in prison if you do not know if they have committed an offence? That is of course the liberty/security argument that you are in. The idea that you can evade that dilemma, which is a real one I acknowledge, by a whole set of measures of control orders and so on is not the case. You cannot evade that; but it is of course the case that control orders, tagging, surveillance and that whole range of issues give you more security than you would have if you did not have them, but less security than a prison cell.

Q322 Steve McCabe: Could I just ask about post-charge questioning. I think you have said you have got an open mind on it and, in fact, you promised a consultation paper. You did say that you were concerned that one of the problems was that it might

not be possible to bring a charge in the first place and hence the difficulty with it. In what proportion of cases do you think it would not be possible to bring a charge in the first place and, therefore, post-charge questioning would be redundant?

Mr Clarke: I do not think it is really possible to give a percentage. I think it must be the case that the percentage that would result in criminal charges as a result of post-charge questioning would be quite low. We are not against it but I think it would be quite low. As I say, we are looking at this and I think it is a perfectly appropriate thing to look at, but it does not solve the problem if it has not been possible to bring a charge against the person in the first place.

Q323 Steve McCabe: Are you still planning to produce a consultation paper?

Mr Clarke: Yes.

Q324 Steve McCabe: Do you know when?

Mr Clarke: Look, we hope to launch it in the next two or three months. I think, Mr McCabe, it is quite important we have had that consultation before we get to what I call the “codified legislation” next year; so the whole idea is having this as comprehensive as possible. That is why we have our time pressure too, to publish the consultation document.

Q325 Chairman: Is that just in relation to terrorism or all serious crime?

Mr Clarke: We have talked about it in the context of terrorism. It is an interesting question, in relation to a number of the measures we have talked about in relation to terrorism, whether there might or might not be any appropriate steps we can take in relation to serious and organised crime—not general crime but serious and organised crime—and we would consider that too, though it is currently intended that the consultation primarily focuses on counter-terrorism, which is where it comes from, but I think there could be a knock-on effect into other areas.

Q326 Colin Burgon: I have a couple of questions on Part 3 of the Regulation of Investigatory Powers Act. We have heard from Lord Carlile and we have heard from JUSTICE who argue that it should be brought into force. We have also heard from Deputy Assistant Commissioner Clarke, and he was far more guarded in his response on this question. Why have you not brought this particular piece of legislation into force?

Mr Clarke: The short answer is that this part of RIPA was conceived in the expectation that it would only be four or five years before all electronic communications and all stored electronic data would be routinely encrypted, and that, in fact, has not happened at the speed at which we anticipated when the RIPA bill was passed. There are a lot of reasons for that, and the technological change is moving very quickly indeed in the whole of the communications field. It is also the case that the abuse of encryption by terrorists and criminals has not taken place at the speed at which we thought it would when the RIPA bill was passed. The take-up of encryption software has been low because a lot of

21 March 2006 Rt Hon Charles Clarke MP

is still very difficult to use properly. I do not know if you have ever tried, Mr Burgon, to use encrypted communications yourself?

Q327 Colin Burgon: No, I have not.

Mr Clarke: There are commercially available options, but in fact it slows down your operation. If, as I am sure you are, you are a very fast one or two finger typist—

Q328 Colin Burgon: I am at the cutting edge of technology: I use Teletext!

Mr Clarke: I thought, as a Yorkshire man, you would be bound to be ahead of the game in this instance! Joking aside, the fact is that there are a lot of people who might think of using encryption but do not, for that reason. It simply has not moved as quickly. We did create the National Technical Assistance Centre, from which you have had evidence in 2001, to provide technical support, and it is doing that, but we would consider that the bringing in of Part 3 is necessary as the situation operates. We will, I think within the next three months, be consulting publicly on a draft code of practice on Part 3 of RIPA and, after that public consultation, Parliament will be required to approve the statutory code. That is the reason why we have not done it thus far, but we think things are moving so that we should deal with it now.

Q329 Colin Burgon: The penalty under Part 3 of RIPA for failing to release an encryption key is two years. Do you think that is inadequate in the light of the fact that the suspect could be facing something like 20 years in prison on a terrorism charge? How do you balance that one out?

Mr Clarke: I do, and that is why we put the proposal in clause 15 on the Terrorism Bill to increase the maximum in national security cases to five years, for exactly the reason you imply, because the encryption key is so important that it needs to be seen as a very serious offence. Some might argue that five years is itself not long enough, but we are increasing it to five years for the reason that you have said.

Q330 Mrs Dean: JUSTICE have proposed that greater attention should be given to the “threshold test” in section six of the Code for Crown Prosecutors, which they consider means that the CPS can bring a charge on reasonable suspicion (ie the same level required for an arrest), but the police have disputed this, arguing that the “threshold test” was not applicable to terrorist cases. Could you tell us your view?

Mr Clarke: At the moment, as you say, Mrs Dean, as regards decisions on charging a government by the DPP’s guidance and to charge under the full code test, which is the one that is likely to be applicable in these kinds of cases, there must be sufficient evidence to provide a realistic prospect of conviction, and also it must be in the public interest to proceed. Both have to be there. The nature of the terrorism we face means that it may be necessary for the police to intervene at an earlier stage than they might have done in the past since intelligence may well link a

person with terrorism, justifying the arrest, but there may not be sufficient admissible evidence at that point to bring a charge and we need to ensure that the police can hold the suspect for a sufficiently long period to enable such evidence to be obtained. That is why we have taken the approach we have, and I think it is the right one.

Q331 Mrs Dean: You have raised difficulties with each of the possible alternatives to extended detention; but is it not possible that cumulatively they would be effective enough for extended detention to be unnecessary?

Mr Clarke: They certainly make it less necessary. The classic example is the new offences in the Terrorism Bill, which I hope will become an Act, which deal with that. It makes it less necessary, but I do not think it makes it unnecessary. What all those cumulative things do is make detention a necessary thing for fewer and fewer people. We have said all the time that we expect it will be a relatively small number of people, and the changes reduce that number of people but it does not reduce it to zero. It does, as you imply, have the effect of reducing the need for it but it does not eliminate it.

Q332 Mr Clappison: Can I move on to the question which you have just raised of the need for early arrest. As part of our evidence we heard from Assistant Commissioner Hayman that there are “a vast amount” of cases now where an early interdiction is to disrupt on the grounds of public safety. I believe it has always been part of the case in support of extended detention that a relatively early arrest is needed in order to prevent some terrorist incidents with the potential for greater catastrophe than in the case of many other types of crime. Does that remain part of your thinking? Would you agree that that is the main case for extending detention?

Mr Clarke: It has always been the case, as you rightly say, but I think the “always” is given increased intensity by the fact you are now talking about suicide bombers rather than people who are setting bombs elsewhere—it puts a different context for that—but you have correctly summed up our thinking. It is critically important for us to disrupt any terrorist attack, and that may involve arresting some people earlier than would be ideal because we need to disrupt the terrorist cell. Nevertheless, the purpose of the arrest is still with the aim of gathering the evidence to bring a charge. All the time it has to be based on seeking to bring a charge—that is the core of the whole thing—but, as always, the police and prosecution have a judgment to make about the appropriate time to make such an arrest, and that is formed, as you rightly say, by the new circumstances which we are up against.

Q333 Mr Clappison: Drawing a distinction on those grounds between this type of arrest and the arrest which is made in other types of criminal case, would you be open in your thinking to consider different treatments of the arrest process through judicial oversight, perhaps, for example, through judicial

21 March 2006 Rt Hon Charles Clarke MP

oversight from before the point of arrest, which is what I believe happens in France and a few other places?

Mr Clarke: I have said before publicly (and I have always got to be careful what I say because I am now speaking on behalf of myself and not the Government), I think that a supervisory system and investigating magistrates regime is very superior to the system that we have in this country. That is not the position of the Government, I make clear. As I say, that is my personal view, but I do not think counsel must swathe themselves in distinction and I do not think the adversarial system has been a particularly effective means of securing justice, but, I admit, I am not a lawyer and, therefore, not steeped in the conventions which say that what I have just said is a load of nonsense, but many of my colleagues in government, as in Parliament, are lawyers who believe that the current system is perfect.

Q334 Mr Clappison: You will be aware there is a high profile case in France at the moment where they are actually looking at this whole issue because of the difficulties which have arisen in the course of the investigation, but my point put to you was looking at what happened before the arrest took place. Would you be prepared to at least think about some judicial oversight, whether on our model or on the Continental model?

Mr Clarke: Yes, indeed. To answer your question directly, yes, I would. I am ready to look at it, but I do not want to give the impression that it is the Government's position that we should go down that course, because it is not. I think there is a lot to be said for it and I think our system would benefit from that, but you will understand, Mr Clappison, better than I, and it would be perhaps surprising to describe Lord Carlile as a revolutionary but actually it is a revolutionary suggestion for our legal system to operate in that way. That does not mean it is wrong, but it does mean that there is not consent for it across the whole of government.

Q335 Gwyn Prosser: Home Secretary, you have been talking about judicial oversight, et cetera, and you have said yourself that you would accept the need for greater judicial oversight. Why is it that you have not gone as far as Lord Carlile when he talks about a judicial authority, et cetera, and a very structured method of overseeing these matters?

Mr Clarke: Simply because I think there is not yet a consensus across the British legal system that that kind of change would be impossible. As I implied in my answer to Mr Clappison, I am personally sympathetic to what Lord Carlile is saying and to the implication of your question, Mr Prosser, right now. I am absolutely open to moving in that direction, but there is not a consensus that that is the right way to proceed.

Q336 Mr Prosser: You have seen that in the evidence that we took from various witnesses there was a very strong view that, because of the adversarial nature of our system, this meant that the decision of district judges was influenced only by the prosecution case

and there was not the opportunity for someone representing the detainee to put his or her case and, consequently, it has been described as a rubber stamp mechanism. We know from our visit to Paddington Green, and from other evidence, that in all of the cases that have come before district judges never has a district judge said, "No", detention is not allowed. We know there is an argument that the case might be very good, but there is a matter there to discuss, is there not?

Mr Clarke: You are quite right, Mr Prosser, to identify those who make that argument. I think the argument is totally wrong and totally flawed. I certainly believe that the courts and the judiciary take these issues seriously. Moreover, I believe that the police work on the basis that the courts and the judiciary take these things very seriously indeed and that they have to be properly carried through. I do not just think it is a question of the defence that the judiciary take it seriously, the police work on the basis that the judiciary takes it seriously and so I simply do not accept the proposition that some have made that the judges are essentially rubber stamps for the police. I think that is absolutely not the case.

Q337 Mr Winnick: Do you think that your proposals to replace district judges with High Court judges would make things fairer?

Mr Clarke: That is a hard question. We accepted, as the government, the view in the Commons that we ought to have this done by a High Court judge, and I accepted that because of the confidence that is reposed in High Court judges. I was slightly reluctant to do so because I thought that implied a lack of confidence in district judges, which I do not believe would be warranted. I think district judges have at least as much integrity and professionalism as High Court judges. You put the question: is it fairer? I would not say it is fairer. I do not think that that High Court judges will be fairer in their approach than district judges, but I accepted the amendment because I accept it would give people more confidence in the integrity of the system, though I myself think that the change was not necessary to give that confidence, if I can put it like that.

Q338 Chairman: Home Secretary, you have often in the course of the discussions about this prayed in aid Lord Carlile's support for the maximum of 90 days detention. Lord Carlile said that his support was based in part on the knowledge of one particular case which had influenced him. The Metropolitan Police and ACPO were not able to give us the details of that case because it was in another jurisdiction, we presume Scotland. Are you familiar with the details of the case that influenced Lord Carlile?

Mr Clarke: I am familiar with the detail of cases. I would not necessarily say that I know which case has particularly influenced Lord Carlile.

Q339 Chairman: Even though that is pretty central to his position?

21 March 2006 Rt Hon Charles Clarke MP

Mr Clarke: I have occasional meetings with Lord Carlile, not regular meetings, but I have not in any such meeting asked him what it is in particular that has led him to his view and, therefore, I cannot comment on that directly.

Q340 Chairman: That might be surprising, Home Secretary. You have very often referred to Lord Carlile's support for the 90-day detention. We thought it a fairly obvious question to ask him why he came to that view. You have not specifically asked him why he came to that view?

Mr Clarke: Not in terms of specific cases, no. I have a high regard for Lord Carlile. I read his published reports very carefully and, as I say, I have an exchange of views from time to time, but I am also conscious, I should say, I do not particularly want to be thought to be unduly influencing him in his judgments because actually his independence is an important aspect of this whole procedure.

Q341 Chairman: We have currently got a maximum of 14 days. Perhaps it was of some comfort to us, but neither the Met or ACPO could point to any instances at all where they believed that they had released somebody who they would have been able to charge with a terrorism offence had they been able to detain them longer. Are you aware of any cases where somebody has been released because they came to the maximum 14 days, where they really, in your view, could in future be charged with terrorist offences?

Mr Clarke: No, I am not aware of any particular case. I am aware of the possibility of such cases, but I am not aware of any particular case. I considered it my duty to put before Parliament changes which were looking to the future rather than changes based on a particular case that had arisen in the past.

Q342 Chairman: Given that the proposal for a maximum of 90 days is a very radical change in our judicial and legal system which the Government is prepared to push ahead with, can you say a little more about why you are so reluctant to bring about the more wide-ranging changes in judicial oversight of the system which you have talked about earlier? I think you said that we cannot have a more judicial oversight because there is no consensus in the legal system about this?

Mr Clarke: I did not say I was reluctant, I simply said there was not consensus and it was difficult to bring about a change. Mr Denham, you have a well-deserved reputation for radicalism and challenge and, if your Committee accepted your lead in this and proposed major changes in this area, I am quite sure that would be taken very seriously by Parliament, and certainly as Home Secretary I would say it would be a good thing if that debate was to be prosecuted.

Q343 Chairman: You obviously believe that the pre-charge detention is compatible with the European Convention on Human Rights because you have signed that declaration on the bill and so

on, but a different point has been put to us that no court is minded to accept as evidence a confession or information volunteered after somebody had been detained for more than 14 days. The courts have always been reluctant to take evidence where people have been detained for a long period of time. Do you believe that is the right judgment?

Mr Clarke: I do not accept that, as a matter of fact. A lot of people make assertions about what courts will or will not do. In fact a very large number of lawyers are paid very large amounts of money to speculate on what courts may or may not do in certain circumstances. I prefer to see the outcome of the courts, and my experience of the courts since I have been Home Secretary is that they have tried to take the right decisions based on the balance of evidence in front of them in accordance with the law, and that is what they will seek to do. I do not think anybody should presume to prejudge what they would do in particular circumstances, and I certainly do not. There are occasions on which I get legal advice which suggests that the courts will not take a particular act and actually they do something opposite to what that advice says. That is what the courts do, and I think that is right. I also think it is the case that the courts are acutely conscious of their own role in relation to this counter-terrorism issue. I think they might well have preferred not to be as involved as they are in some of the processes which we have here, and there are issues for them in that, but I see absolutely no evidence that the courts will not (a) take it very seriously and (b) look at any evidence that arises in the way you have described very seriously. It is possible, as you say, that when they do so they would not accept evidence based on detention for longer than 14 days, but it is only possible and I certainly do not assume that that would be the case.

Q344 Mr Winnick: Home Secretary, in your reply to a question from my colleague, Mr Malik, you made, rightly of course, the point that one should not associate Muslims with terrorism any more than in the past one associated the Irish with the murderous attacks which were made upon us over 30 years, recognising, of course, that Muslims are quite as likely to be the victims of terrorism as the rest of us, as was shown by what happened on 7 July. The question I want to ask you is: do you know of any representative Muslim organisations which support 90 days detention?

Mr Clarke: I am not aware of any off-hand, but I would need to double check my answer to you, Mr Winnick.² Certainly the main one, the Muslim Council of Britain, opposed it.

Q345 Mr Winnick: I am a bit surprised when you say you do not know of any off-hand. I would have thought, if you did know of any, you would have used that as supporting evidence in the Chamber and obviously now?

² Ev 102

21 March 2006 Rt Hon Charles Clarke MP

Mr Clarke: I would need to go back to my speeches in the Chamber, which is something I sometimes do late at night for relaxation.

Q346 Mr Spring: So do we!

Mr Clarke: I am not sure whether Mr Spring is saying he is going back to his own speeches or back to my speeches! I do not recall in general, with the important exception of the police and security services, relying on support from particular bodies of opinion in making the case I sought to make the argument on its own terms but I will go back and look at the particular point.

Q347 Mr Winnick: It is an important point. If we all accept that the overwhelming majority of Muslims are as much opposed to terrorism as we are, if there were mainstream organisations representing Muslims one would have thought they would let you know, broadly speaking, that they are supportive of what you intended to do.

Mr Clarke: Again, some of the mainstream Muslim organisations are concerned principally with the standing, status and the issues facing the Muslim community in this country of which terrorism is only one. It is not even central to some organisations.

Chairman: Home Secretary, thank you very much indeed for the clarity and the comprehensiveness of your answers.

Written evidence

Asterisks in the written evidence denote where part of a document has not been reported, at the request of the submitter and with the agreement of the Committee.

1. Joint memorandum submitted by the Association of Chief Police Officers of England, Wales and Northern Ireland (ACPO) (Terrorism and Allied Matters) Committee and the Metropolitan Police Service

This submission should be seen alongside the more detailed proposals submitted by Assistant Commissioner Andy Hayman with his letter to the Home Secretary on 6 October.

The October document sets out the case for extension of pre-charge detention by judicial review and argues the case for extension given the complexity of international terrorism investigations requiring early interdiction; the unfolding sequence of enquiries and sifting of considerable evidence by thorough and painstaking investigation.

This submission contains our observations on the alternative proposals and offers the arguments that we would wish the Committee to consider.

We will, of course be willing to assist the Committee further and hope that you will draw on the expertise on counter-terrorism within ACPO (TAM) and the Metropolitan Police Service.

1. SPECIFIC ARGUMENTS PUT FORWARD BY THE POLICE IN SUPPORT OF EXTENDED PRE-CHARGE DETENTION

1.1 In support of judicially sanctioned, seven day extensions of pre-charge detention up to a maximum of 90 days, the Police Service has stated the case for extending pre-charge detention for terrorist cases. These arguments were set out in Assistant Commissioner Andy Hayman's letter to the Home Secretary on 6 October 2005. The case put forward remains the same and the police have nothing further to add at this stage.

2. JUDICIAL OVERSIGHT

2.1 We are disappointed that the recent debate on our proposal to extend detention for some terrorist suspects has focused on a maximum limit of 90 days, as opposed to our strong position of extending detention in excess of 14 days, where necessary, through judicially approved seven day periods. As has already been accepted, extensions past seven days are used very infrequently and only then against those suspected of serious terrorist offences. Therefore, the focus on the maximum period is both unhelpful and misleading.

3. POSSIBLE ALTERNATIVES TO EXTENDED DETENTION POWERS

3.1 This submission will focus on the possible alternatives to extending detention powers, on which ACPO have not yet afforded a view, unlike the extended detention pre-charge debate.

3.2 The police have reviewed the alternative proposals suggested and conclude that, although each alternative could be a useful tool in the fight against terrorism, they are not an adequate replacement or alternative to extending pre-charge detention. None of them will provide satisfactory safeguards when dealing with those terrorists determined to carry out the kind of atrocity experienced in July.

3.3 All the alternatives to extended detention suggested are resource intensive and may divert resources away from the investigation in order to operate the alternatives.

4. CONTEXT

4.1 Before discussing the possible alternatives to pre-charge detention, we feel it is useful to restate the very real terrorist threat now facing us.

4.2 The threat today is very different to that of the past, the terrorist challenge has changed.

4.3 As was set out in Assistant Commissioner Hayman's letter of 6 October 2005, "The threat from international terrorism is so completely different that it has been necessary to adopt new ways of working. The advent of simultaneous terrorist attacks designed to cause mass casualties, with no warning, sometimes involving the use of suicide, and with the threat of chemical, biological, radiological or nuclear weapons means that we can no longer wait until the point of attack before intervening. The threat to the public is simply too great to run that risk."

4.4 In the interests of public safety, we are now compelled to disrupt terrorist activity much earlier than before. This will normally involve arresting suspects where the necessary evidence to support charges reflecting the seriousness of the terrorist intentions is yet to be understood.

4.5 As Chief Constable Ken Jones, Chair ACPO Terrorism and Allied Matters committee stated to the Joint Committee on Human Rights in October 2005:

“the fundamental difference is that we now have people prepared to use suicide as a weapon and have an ideological motivation rather than as a purely political motivation which we have seen in other forms of terrorism. The other thing that has changed is that the organisation of terror is different. It is shapeless, it is amorphous and it is constantly changing and that is not inside our recent experience. That is a fundamental difference, the suicide issue and the ideological issue.”

5. PROVIDE MORE RESOURCES TO THE POLICE AND INTELLIGENCE SERVICES

5.1 Although the Police Service naturally welcomes, and is increasing counter terrorism resources, the challenges presented to the Service by international terrorism must be met with the capacity to act swiftly and effectively with expertise and diligence, rather than with a mass deployment of personnel and equipment.

5.2 The complexity of the investigative process, the sheer volume of intelligence and seized material, and the international dimension common to all modern terrorism operations require a methodical, sequential investigative process that places the onus on the quality of the work undertaken rather than the quantity of resources deployed. This cannot, as DAC Peter Clarke, Head of the Anti-Terrorist Branch said, be a “cavalry charge”.

5.3 Terrorist investigations form a complex sequence of inter-related activities beginning with the intelligence, evidence or events coming to notice, then progressing through meticulously recorded stages of retrieval, logging and assessment.

5.4 Many investigative procedures, technical analysis and forensic processes are the preserve of highly skilled law enforcement and specialist agency personnel. They are inherently time consuming for scientific reasons or because only a limited number of people can ensure safety and continuity of the task at any given time.

5.5 In order to identify the most productive strategies for interviewing suspects and furthering the investigation, it is necessary to establish a clear picture from the myriad of sources of information and utilize the value of verified forensic data. The Senior Investigating Officer and a small, dedicated team complete this task. Anything more than this can create confusion and the possibility of important evidence being missed.

5.6 During the Joint Committee on Human Rights on 24 October 2005, Deputy Assistant Commissioner Peter Clarke was asked about this specific point by Dan Norris and his answer is still as relevant.

Dan Norris: “Is it fair to say that some increase in resources would help and therefore perhaps the three-month detention period is too long?”

Peter Clarke: “No, it would not. However many resources we had I do not think it would cut into the basic problem here, which is the sheer weight of material which we are routinely recovering in these cases. This has to be analysed at some point and then focused into an interview strategy and an investigation strategy set by the senior investigating officer. At some point one person has to be aware of what is emerging from all this data. It cannot just be a cavalry charge.”

6. BRINGING LESSER CHARGES TO ENABLE TERRORISM SUSPECTS TO BE HELD IN CUSTODY WHILE THE MAJOR INVESTIGATION PROCEEDS

6.1 We believe there are a number of problems with the suggestion of charging for a lesser offence as an alternative to extending the period of detention.

6.2 With the onset of statutory charging in England and Wales, the emphasis is on both the Police and Crown Prosecution Service working together as a “prosecution team” to ensure that the person is charged with the right offence from the outset, according to the evidence obtained. Not doing so is contrary to this important change in the Criminal Justice System.

6.3 There is no guarantee that there will be sufficient evidence to charge with a lesser charge in all cases. Terrorist suspects are being arrested at a much earlier stage than before due to public safety. Although there will be grounds to make the arrest, this does not mean there is evidence to charge. Evidence may not become available until forensic analysis and computer evidence, for example, is obtained and that invariably takes time.

6.4 Concentrating on a lesser charge would unnecessarily divert focus and resources away from fully investigating the offence for which the person had been arrested.

6.5 Additionally, in order to allow a remand in custody to investigate terrorist offences, there would need to be a change in the law, as the investigation of another offence, for which someone is not currently charged, is not a legitimate reason for remanding a defendant in custody or delaying proceedings.

6.6 Whereas an extension of detention would have robust judicial oversight every seven days, a remand in custody to allow further investigation into the terrorist offence would not have the same level of scrutiny and the defendant could spend longer in custody than necessary—the reverse intention.

6.7 The lesser offence might not justify a remand in custody.

6.8 The defendant may be advised to plead guilty and could be released unless the offence was serious enough to attract a custodial sentence, or their conviction history would justify it. This would allow a potential terrorist to walk free and pursue activities unhindered.

7. USE OF TAGGING, SURVEILLANCE OR CONTROL ORDERS AS ALTERNATIVES TO CUSTODY

7.1 Due to the nature of terrorism today and early intervention in order to prevent unnecessary loss of life, the use of tagging, surveillance or control orders are simply not an alternative to detention in the most serious of cases. Many terrorists today are willing to take their own lives and those of others as we saw in London on 7 July.

7.2 Tagging allows Police to monitor the suspect and identify whether they breach their curfew. Tagging could not prevent a suspected terrorist from committing an act of terrorism or from removing their tag and fleeing the country.

7.3 The Home Secretary may make a Control Order (with permission of the court, renewable after 12 months) if he has reasonable grounds for suspecting that an individual is or has been involved in terrorism-related activities and is satisfied that it is necessary to make an order for the purposes of protecting members of the public from terrorism. A control order is likely to be made, for example, when there is no likelihood of an individual being charged with a terrorist offence. Derogating control orders (ie those where the obligations imposed are incompatible with Article 5 ECHR) can only be made by the court.

7.4 Whilst control orders may be effective against those suspects on the periphery of terrorism, and may provide the adequate form of control that is required, they are not an alternative for those suspects that have been arrested for serious terrorist offences. Control orders do not replace detention as the ultimate measure for protection.

7.5 Monitoring and surveillance are highly resource intensive and in order to be successful and to minimise the risk to the public it would require a team of police officers watching a person 24 hours a day, seven days a week. Not even that level of control would ensure the prevention of a suspect from planning or carrying out an attack. This is simply not practicable.

8. POWER TO QUESTION TERRORIST SUSPECTS AFTER CHARGES HAVE BEEN BROUGHT

8.1 The Police Service welcomes the decision by Government to examine whether there is any possibility of extending generally the ability of police to conduct interviewing post charge.

8.2 There are, however, a number of problems with this being considered an alternative to extended detention in terrorist investigations.

8.3 The detention process is not about interviewing alone as many people do not answer questions in any event. It is about a structured investigation and interview strategy, doing things in the most effective way and questioning, when the evidence has been obtained and assimilated, for maximum effect and maximum inference if the suspect fails to answer.

8.4 At present, a suspect cannot be interviewed about an offence after they have been charged unless the interview is necessary, for example, in the interests of justice, for the detainee to have put to them, and have an opportunity to comment on, information concerning the offence which has come to light since they were charged.

8.5 In order to be able to question suspects further after charge, a charge must first of all be preferred. As already stated, this is often one of the difficulties complex terrorist cases present. It may not be possible to collect all the evidence to charge someone with an appropriate offence within the permitted time.

8.6 Any interview must be voluntary. In the majority of suspect interviews, terrorist suspects are advised, and exercise, their right to remain silent, from which no adverse inferences can be drawn. This is because the offence for which they have been charged is no longer being investigated and the caution under section 34 Criminal Justice and Public Order Act 1994, relating to adverse inferences, is not applicable. This provision, however, may be changed following a Government review of the position.

9. PERMITTING THE USE OF TELEPHONE INTERCEPT EVIDENCE IN THE COURTS

9.1 In relation to our ability to investigate terrorist offences, we welcome any development, which will allow us to put more evidence before the courts.

9.2 From the ACPO perspective, there are three key issues:

- best evidence should always be sought and, in some circumstances, that includes intercepted communications;
- ACPO should move to a position where a selective approach to the evidential use of intercepted communications can be taken, with some areas excluded; and

- the opportunities involving interception of communications currently available should be better exploited. This would require higher levels of investment than currently exist.

9.3 A group within ACPO is reviewing the intercept issue. The Group includes representation from the CPS and all the Security Services.

9.4 The purpose of the ACPO working group was to develop guidance on interception of communications as a law enforcement technique and identify opportunities for enhancing current and future use by police; this will include advising in respect of appropriate legislation and other matters.

9.5 The perspective was that there are a number of specific problems to be overcome:

- In respect of disclosure, this issue is currently being worked on by the CPS and in many respects is catered for in the decision in the case of “*R v H and C*”.
- Delivery of Foreign Language interception translation to an evidential standard given the difficulties in securing adequately vetted listeners.
- Delivery of product to an evidential standard in the voice over internet environment subject to the technical difficulties, which are still to be overcome.
- Security issues currently being worked on by the Home Office led Intercept Advisory Group.
- ACPO do not see any differentiation between the use of interception in relation to serious crime and terrorism.

9.6 Pre-emptive arrests made as a direct result of intelligence has meant that many investigations do not have the time frames to use intercept as an investigative tool. Therefore allowing intercept as evidence within the court will only be of value to those cases where we have been in a position to obtain such evidence before arrest.

13 December 2005

2. Memorandum submitted by British Irish Rights Watch

1. INTRODUCTION

1.1 British Irish Rights Watch (BIRW) is an independent non-governmental organisation that monitors the human rights dimension of the conflict and the peace process in Northern Ireland. Our services are available free of charge to anyone whose human rights have been affected by the conflict, regardless of religious, political or community affiliations, and we take no position on the eventual constitutional outcome of the peace process.

1.2 We welcome the opportunity to make a submission to the Home Affairs Committee inquiry into the police case for an increase in detention powers in respect of terrorism suspects. We have only commented on those issues which fall within our remit.

2. HUMAN RIGHTS AND THE EXTENSION OF PRE-CHARGE DETENTION

2.1 The case, put forward by the police, in support of 90-day pre-charge detention is ultimately flawed. It ignores the international human rights treaties and conventions to which the UK is a signatory. These include the European Convention on Human rights (ECHR) and the UN Convention against Torture (CAT).

2.2 The extension of pre-charge detention contravenes Article 5 of the ECHR, which states:

“Everyone arrested or detained in accordance with the provisions of paragraph 1(c) of this article shall be brought promptly before a judge or other officer authorized by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial.”¹

This violation has been noted in a previous submission to the Joint Committee on Human Rights by BIRW and by other human rights organisations. If the case against an individual is being constructed while that individual is in custody, it is unlikely that he or she will be promptly charged with an offence.

2.3 Article 3 of the ECHR states:

“No one shall be subjected to torture or to inhuman or degrading treatment or punishment.”²

BIRW argues that extended detention times constitute inhuman treatment. The psychological implications for the detainee, who may be held for up to three months without any charge being put to him or her, are severe. This psychological pressure may lead to self-incrimination, false confessions, self-harm and suicide attempts. British Irish Rights Watch has seen testimonies from detainees in Northern Ireland, who were often held for up to seven days; these clearly illustrate the psychological pressure brought to bear

¹ *European Convention on Human Rights*. <http://www.hri.org/docs/ECHR50.html>

² *European Convention on Human Rights*. <http://www.hri.org/docs/ECHR50.html>

by extended detention. In particular extended detention can lead to an increase in the consumption of anti-depressants, development of a limited appetite and weight loss. If detention for only seven days can have such effects, then the effects of detention for 90 days could be serious and lasting. Recent television pictures of Abu Qatada, who recently made an appeal on behalf of Norman Kember, who was taken hostage in Iraq, demonstrated that he had lost a considerable amount of weight while in prolonged detention. Detainees held for 90 days will almost certainly lose their jobs and their education may also be disrupted. For the family of detainees the consequences may be psychological, social, and financial. Extended detention would also breach Article 8 of the ECHR, which protects the right to family life.

2.4 Article 16 of the CAT states:

“Each State Party shall undertake to prevent in any territory under its jurisdiction other acts of cruel, inhuman or degrading treatment or punishment which do not amount to torture as defined in article I, when such acts are committed by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity.”³

BIRW believe that extended detention would contravene this article. Individuals held in the same police station for a prolonged period of time may be more susceptible to acts of cruel, inhuman or degrading treatment by custody officers unfamiliar with the special needs of prolonged detention. Police custody officers are not trained prison officers, nor are they aware of the many issues which arise from extended detention. Even with appropriate training, police stations lack the basic facilities required for detention of this nature.

2.5 Article 6 (1) of the ECHR says:

“In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. . .”⁴

BIRW believe that an individual held for three months prior to charge will not have a fair and public hearing. As noted above, the desire to end detention, perhaps by “confessing” or some other form of self-incrimination could contaminate the case. The admission of such evidence may ultimately lead to the case being dismissed. This could have security implications for the UK. If a case collapses for these reasons, it could also lead to civil action by the detainee.⁵ Furthermore, the mere fact of detaining a suspect for such a long period of time could undermine the presumption of innocence; the public perception of someone held for such a long time is likely to be that there is no smoke without fire. Such social stigma can also attach to the detainee’s family.

2.6 Those individuals subject to extended pre-charge detention occupy a legal vacuum. The absence of a charge against them ensures they can not be progressed to the stage of either being released on bail, or remanded in custody in a prison. The absence of this latter stage is particularly problematic. Individuals remanded in custody are subject to the same standards, for the most part, as convicted prisoners. International human rights standards such as the Council of Europe’s Prison Rules (revised) clearly outline the conditions suitable for individuals in detention. These include making provisions for access to religious representatives, and necessary books/literature for religious practice.⁶

2.7 Ninety-day detention is, in our submission, internment without charge by another name. As a human rights group focussed on Northern Ireland, we can only remind the government that internment without trial was introduced there at the start of a long and appalling conflict that is not yet resolved. We have seen the negative impact of internment in Northern Ireland. This policy wrongfully imprisoned hundreds of people, based on faulty intelligence, and directly contributed to increased IRA recruitment. It has been our experience that repressive laws do not defeat terrorism, they merely create miscarriages of justice and martyrs to the cause. If we react to terrorist attacks by enacting ever more draconian measures, there is a real and present danger that we will undermine our own democratic society, and to that extent we will have assisted the terrorists in achieving their aims.

2.8 The debate around counter-terrorism measures has, in our view, largely been based on a false dichotomy between the need to protect society, on the one hand, and the need to protect human rights, on the other. The strongest possible defence against terrorism is a robust system of human rights protection. Developing such a system both decreases the likelihood of producing “home grown” terrorism, such as we saw in July 2005, and enhances the likelihood that the communities within which terrorists live will be prepared to provide the vital intelligence required to prevent and detect terrorist crimes.

2.9 BIRW also believes that it is a mistake to create a separate set of laws for terrorist cases. All the crimes committed in the name of terrorism—such as murder, hijacking, illegal possession of weapons and explosives, etc—are already crimes under the ordinary criminal law, which is perfectly adequate for dealing

³ *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*. http://www.unhcr.ch/html/menu3/b/h_cat39.htm

⁴ *European Convention on Human Rights*. <http://www.hri.org/docs/ECHR50.html>

⁵ In Northern Ireland, the vast majority of those arrested on terrorism charges were subsequently released without charge.

⁶ *Recommendation No R (87)3 of the Committee of Ministers to Member States on the European Prison Rules*. Note: these have recently been revised. <http://www.iuscrim.mpg.de/info/aktuell/lehre/docs/EUPrisonRules.pdf>

with acts of terrorism. Creating a twin-track legal system, which gives those suspected of involvement in terrorism less rights than other suspects, poses the danger of elevating terrorism in the eyes of some and, indeed, glorifying it.

3. THE POLICE CASE FOR EXTENDING DETENTION TIME

3.1 British Irish Rights Watch believe that the case put forward by the police, as outlined in a letter from Assistant Commissioner Andy Hayman to the Home Secretary, is inherently weak.⁷ BIRW firmly believe that a person should not be arrested without reasonable grounds. We do not think it is appropriate to arrest an individual and then seek the grounds which should have been established before the arrest.

3.2 The police assert that the role of international networks in contemporary terrorism is problematic, since reliance upon other law enforcement and judicial authorities, scattered globally, hinders effective and prompt police investigation. However, such an assertion ignores the post-9/11 steps taken to promote international co-operation in criminal investigations, most pertinently in terrorist investigations. British Irish Rights Watch does not believe that the way to address cross-jurisdictional issues lies in the introduction of draconian domestic legislation. Rather, the UK government should be utilising and strengthening international mechanisms and processes for extradition, information sharing, and cross-border policing.⁸ The UK Government should also draw on its experience of combating IRA terrorism, which utilised international networks for funding and weaponry, and implement the lessons learned.⁹

3.3 The principle of increasing collaboration in police investigations can be applied to mobile telephone companies. The Assistant Commissioner states, "Obtaining data from service providers and subsequent analysis of the data to show linkages between suspects and their location at key times all takes time."¹⁰ If so, then the resources must be provided to develop faster technology.

3.4 BIRW has previously acknowledged a need for the use of telephone intercepts in terrorist investigations. However, we have always emphasised that careful attention needs to be paid to the human rights implications of covert surveillance, in particular its impact on the privilege against self-incrimination. Care also needs to be exercised in targeting suspects for such surveillance because of its impact on the right to privacy, not only of the suspects but of third parties. If intercepted communications are to be allowed in evidence, then so too must information about how such evidence was obtained, in order that the defence may challenge evidence that was gathered improperly. The use of intercepted material which is shrouded in secrecy because of an alleged need to protect sources and methods is not acceptable.

3.5 The use of telephone intercepts should be the subject of keen safeguards; with a rigorous system for approval. British Irish Rights Watch believe that such intercepts should be used for the minimum amount of time necessary and therefore be subject to regular review, with a view to removing them at the earliest opportunity. A system which enables individuals to find out if their telephones or other means of communication, such as e-mail, are tapped, and to subsequently challenge such surveillance, should be put in place and must be robust and transparent.

3.6 The Assistant Commissioner draws attention to the fact that one firm of solicitors represents the majority of terrorism suspects detained. Our experiences in Northern Ireland indicate that, while the number of solicitors representing suspected terrorists was relatively limited, this did not have an impact upon investigations. Rather, the attitude of the police towards the solicitors, and their ability to access and take instructions from their clients, violated the rights of the detainees and also their solicitors, many of whom were abused and threatened by police officers before safeguards were introduced to prevent such abuse.¹¹ BIRW would strongly caution against any restrictions placed upon contact between lawyers and their clients, under the guise of hastening a criminal investigation.

3.7 The crux of the Assistant Commissioner's arguments appear to be centred on a lack of resources, but he also argues that increased resources would not reduce the time taken by pre-charge procedures.¹² BIRW disagree with his approach. On matters such as the need to employ interpreters, increasing financial and personnel resources will undoubtedly help. BIRW acknowledge that the presence of rare languages and dialects as the primary means of communication for a percentage of terrorist suspects is problematic. However, the Assistant Commissioner appears to be ignoring the highly multi-cultural nature of Britain's cities; where interpreters are used across a wide range of public services. BIRW would also draw attention to the use made by the British army of UK university students; who were persuaded to put their degrees on

⁷ Letter from Assistant Commissioner Andy Hayman to the Home Secretary, 6 October 2005. Courtesy of the Home Affairs Committee.

⁸ The UK government does need to be mindful of the evidence received from states who are known or suspected to practice torture. In particular considering the case of A and Others, of which addresses the use of "torture evidence". The judgement in this case can be found at: <http://www.publications.parliament.uk/pa/ld199697/ldjudgmt/ldjudgmt.htm>

⁹ Suspected IRA terrorists were training FARC guerrillas in Columbia. See *IRA influence in FARC attacks*. BBC News online. 9 May 2005, and *FARC-IRA link "cannot be ignored"*. BBC News online. 8 September 2005.

¹⁰ Letter from Assistant Commissioner Andy Hayman to the Home Secretary, 6 October 2005. Courtesy of the Home Affairs Committee.

¹¹ Two solicitors, Patrick Finucane and Rosemary Nelson, were murdered because of their work defending terrorist suspects.

¹² Letter from Assistant Commissioner Andy Hayman to the Home Secretary, 6 October 2005. Courtesy of the Home Affairs Committee.

hold to translate for the army in Iraq.¹³ An increase in resources would also contribute to the development of faster decryption of computers and hard drives as well as increasing forensic examination capacity. BIRW believe that increasing resources should not be as swiftly dismissed as it appears to have been here.

3.8 BIRW do not agree with the argument that religious observance delays investigations. Nor are we comfortable with the racial and religious profiling the Assistant Commissioner appears to be employing. We understand that the average prayer time for Muslims is approximately seven minutes, including the cleansing ritual, five times per day.¹⁴ We find it hard to believe that 35 minutes of religious observance per day can delay a criminal investigation. Affording prisoners of any religion the courtesy of allowing them to practice their customs ought to be taken for granted in any civilised country, while depriving people of these rights would rightly be interpreted by the wider community as oppressive and offensive.

4. ALTERNATIVES TO EXTENDING DETENTION POWERS

4.1 BIRW is opposed to the idea of charging suspects with more minor offences to enable the police to continue their investigations. We believe this would contravene the right to due process, and undermine the judicial system. In Northern Ireland, this principle has been applied (either by design or accident) and the result has often meant that suspects have to be granted bail as the time taken to get to trial has been deemed to take too long. In some cases this has enabled suspects to commit further offences.

4.2 BIRW is similarly opposed to the principle of the police being able to continue questioning terrorist suspects after charges have been brought. BIRW believe this could lead to the harassment of detainees. If there is not enough evidence at the time of charging, then no charge should be applied. The vulnerability of detainees should not be utilised to build further cases against them.

5. CONCLUSION

5.1 British Irish Rights Watch encourages the Home Affairs Committee to collaborate with the Joint Committee on Human Rights on the issue of extended detention. Their investigation into detention concluded “that three months would have been clearly disproportionate and, in view of the deficiencies in the procedural safeguards for the detainee, which the original Bill did nothing to improve, would have also been accompanied by insufficient guarantees against arbitrariness.”¹⁵ BIRW agrees with this opinion.

5.2 As we have stated elsewhere, draconian legislation is not an effective method of combating terrorism. The police appear to believe that limiting the application of the CAT and ECHR will serve to enhance their investigations into terrorist activity. As this submission has indicated, the argument for these limits is ultimately flawed.

9 December 2005

3. Memorandum submitted by Campaign Against Criminalising Communities (CAMPACC)

We welcome your inquiry into government proposals to extend the maximum period of detention without charge.

Our campaign were set up in early 2001 to oppose the Terrorism Act 2000, especially the broadened definition of terrorism to include normal political activities and resistance to oppressive regimes abroad. We also opposed the extension of the maximum detention period without charge. Our campaign links human rights campaigners with people targeted by the anti-terror powers and provides practical support for them, eg protest events, letters, bail surety and home visits under control orders. From that experience we have special expertise in the human effects of anti-terror powers, as well as insights into how they are used.

GENERAL COMMENTS ON DETENTION POWERS

Since anti-terror laws extended the maximum detention period to seven days and then to 14 days, these powers have been used for political agendas, not to protect us from violence. They have been used to intimidate and stigmatise people as “terror suspects”, especially refugees, as well as to extract information about political activities, in ways consistent (and predictable from) the UK’s broadened definition of

¹³ *Language students to help army in Iraq*. The Guardian. 18 February 2004.

¹⁴ Though obviously this is impacted by the religiosity of the individual.

¹⁵ *Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters. Third Report*. Session 2005–06. Joint Committee on Human Rights. <http://www.publications.parliament.uk/pa/jt/jtrights.htm>

“terrorism”. These longer periods have helped the police to make arrests before having specific or adequate grounds to bring charges, even deferring a serious investigation until afterwards. The Committee should broaden its inquiry to consider the unofficial reasons for those powers and their actual uses to date.

The 7 July attacks were used as a pretext for new anti-terror powers, including a longer detention period. Yet such powers would not have prevented the 7 July attacks, nor could they prevent such attacks in the future. An even longer maximum period would extend the scope for such abuse of state powers; it would be used to extract real or imaginary “information”, in turn justifying detention of yet more “terror suspects”. It is false problem to “balance” security against liberty, because so-called “anti-terror” powers do nothing to make us more secure from violence, though they can help to protect UK foreign policy from dissent.

In Andy Hayman’s 6 October letter justifying a 90-day detention period, the main specific example given is the so-called “ricin” trial, which he calls “Operation Springbourne 2002–05”. He implies that a longer detention period could have enhanced the prospect of convictions. This example is outrageous, given that the main prosecution evidence was obtained by torturing a detainee in Algeria, who ended up losing some front teeth in the process. The case collapsed because the prosecution had no credible evidence of any ricin, much less of a conspiracy to use it—not because the maximum detention period was too short. Moreover, the no-ricin no-conspiracy case was politically motivated by the need for mass-media scares about WMD in the run-up to the attack on Iraq in March 2003, as well as the need to justify anti-terror powers.

POSSIBLE ALTERNATIVES

The Committee’s call for evidence mentions several alternatives to extending detention powers. Here we briefly comment on each one.

Providing more resources to the police and intelligence services

This has already been done, but for what purposes? If these resources are used even more to persecute refugees (eg based on “information” from torture abroad) or to spy on political activities, then they will do little to protect us from violence. On the other hand, more resources could be used to deter or prevent individuals from carrying out violent activities.

Bringing lesser charges to enable terrorism suspects to be held in custody while the major investigation proceeds

Already anti-terror laws have been used to prosecute ordinary crimes, by implying that they had some link to violence abroad, yet with little evidence. “Bringing lesser charges” could mean extending such abuses of the law.

Use of tagging, surveillance or control orders as alternatives to custody

Already control orders and the 1971 Immigration Act have been used to impose punishment without charge, eg in the form of tagging requirements, deprivation of liberty, etc. These measures are inherently unjust.

Giving the police power to continue questioning of terrorism suspects after charges have been brought

Any arrest should be based on substantial evidence resulting from investigation. If police are authorised to continue questioning a suspect after charge, then this power would guarantee further abuses, especially arrests on arbitrary or political grounds.

Permitting the use of telephone intercept evidence in the courts

This would be justifiable in principle, but such an option could turn out to supplement longer detention periods rather than replace or avoid them. So such evidence would not necessarily provide an alternative.

In conclusion, police (and government) arguments for longer detention periods have no basis in any need to protect us from people planning violent activities. If the police already have such a suspicion about specific individuals, then there are numerous ways to deter or prevent them (without detention), through appropriate use of police resources. The Committee should broaden its inquiry to look at political abuses of the detention powers which already exist.

Estella Schmid
Committee Member

11 December 2005

4. Memorandum from Robert Czapiewski

By way of background, I am a director of ICT Cambridge Ltd, a company setup in January 2004 to specialise in providing a national solution to the challenges faced by UK Police in accessing Call Data Records (CDRs).

We have developed a technical solution to these issues, which we call Shield II. Our system is designed to meet the needs of all parties concerned with call data access—namely the government, police and CSPs. Shield II was designed as a national system to provide all UK police forces with equal access to CSP data rapidly, securely and at low cost.

I have been working on this issue personally since 2002, including eight months in close collaboration with the Telephone Intelligence Unit (TIU) of the Metropolitan Police Service (MPS) to understand fully the issues the police faced and needs they have in this regard. I was formerly in the telecommunications field, which first brought me into contact with the police and the challenges they faced.

I write specifically in relation to oral evidence given to the Committee on 14 February regarding the supply of call data records (CDRs) by Communication Service Providers (CSPs). Ref. <http://www.publications.parliament.uk/pa/cm200506/cmselect/cmhaff/uc910-ii/uc91002.htm>

1. Two issues arose which I feel gave the Committee an inaccurate picture of the way that data could be made available and which might have a bearing on the Committee's deliberations. These are:

- (a) Timely access to call details records.
- (b) Standardisation of call data output.

2. My reason for writing is to make the Committee aware that a solution to these practical issues has existed for some years and that the Home Office has been aware of this work since late 2002. These issues are not new and, although much time, energy and money has been spent discussing and consulting on these problems, the reality on the ground remains much the same.

3. During 2002 and 2003 the Home Office was very supportive of our work and excited at the prospect of the UK taking a lead in providing a national system, which could then be adopted by other countries that face similar problems. These days rapid international cooperation is crucial in combating organised crime and worse. Following a change of personnel in the department responsible, however, the climate and policy changed and currently the Home Office take the view that it is up to each police force and each CSP to decide for itself what, if anything, it wants to do.

4. The policy towards Government funding also changed in 2005, with an obvious shift towards large CSPs as evidenced in the attached Home Office newsletter [*not printed*]. Since the large CSPs already have systems in place to provide police with relevant data and charge accordingly, so the government's focus has been on the retention of data. However, these in-house solutions do not solve the issue of data formatting for police analysis.

5. Although the Home Office has spent a great deal of time on data retention, their current policy regarding funding and data access does not, in my opinion, offer value for money, nor does it solve the problems that police have in getting call data in a rapid, secure and standardised manner.

6. Last summer, in a document provided to the EU Parliament,¹⁶ the Home Office indicated that it had agreed to fund a project for ONE large mobile phone at a cost of £875,000. This would allow the company to retain all its data for 12 months and to provide "a tool to retrieve specific data". For less than that amount we could have deployed our system to all UK police forces and 50 CSPs. The only thing then left for the government to fund would be the data retention by the CSPs.

7. Regarding timely access to CDRs, Mr Parmar states in his answer to Q154 that in the most urgent case of a threat to life: "If it is a level one incident then it is usually within two to three hours or, for the worst case scenario, it would be within 24 hours that the information would be available." And in response to the same question, Mr Smith states: "It is severity that produces those speeds."

In today's world, this is totally unacceptable. This information could be available electronically within minutes, regardless of the "severity" of the case.

A few years ago I was personally involved in helping the MPS with in a "threat to life" kidnap case, in which call data was vital. The successful outcome of the rescue was only achieved because I was processing CDRs within minutes of calls being made and the police were quick to realise that the situation on the ground was different to what they initially believed. There is little doubt that waiting a few hours for data would have cost lives.

8. In relation to the standardisation of call data, in response to Q174, Mr Greener states: "There is a variance between those operators in terms of the level of detail that you get to work on, to analyse, so a standardised, across-the-board output would be beneficial to the analyst and would also minimise the skill set slightly across all analysts so that the data was understood by one and all."

¹⁶ *Liberty and Security, Striking the Right Balance*—Paper by the UK Presidency of the European Union: <http://www.fco.gov.uk/Files/kfile/LibertySecurity.pdf>

Again, this need not be the case. CSPs keep their data in formats which best suit their business purposes, this is perfectly understandable. The police, on the other hand, need the data in certain formats to import into analytical programmes. Much of their time is spent reformatting data, or retyping data which has come to them in a different format, including in hard copy or fax. This can lead to mistakes and is terribly time-consuming.

We provide a solution which allows CSPs to retain their own formatting and at the same time provides police with the data in a common standard format for immediate analysis and a sealed copy of the original data for evidentiary purposes.

9. Our system is fully RIPA-compliant for use in the UK. It would improve police intelligence and cross-border cooperation in line with the Home Office National Policing Plan 2005–08 (s3.55) and would reduce cost and bureaucracy (s5.10-5.12) whilst also meeting Recommendation 3 of the Bichard Inquiry (s4.12, 4.35). Indeed it meets the criteria set out in the EU Directive in Data Retention (February 2006) and can even provide national statistics to the Interception Commissioner as provided for in Article 10 of the Directive.

10. Given the sensitive nature of this subject we have taken a deliberately low profile, but our senior advisor, Sir Hugh Annesley (former Chief Constable of the RUC) recently said in an article for a US intelligence paper: “The Shield II system not only assists investigators to achieve the information necessary to progress their enquiries very quickly, but it does so in tabulated form, even from different service providers. I wish we had had this technology when I was serving in Northern Ireland.”

11. I feel strongly that the Committee should be aware of the existence of our system, which is a technical advancement created in the UK for UK law enforcement. Therefore a national system is, and has been, available to solve the issues of timely access to call data, data standardisation, legal compliance, civil liberties, government oversight and disruption to CSPs. Data is provided in a standardised format, from different carriers, and within seconds or minutes of a properly authorised request being issued.

However, because of the fragmented nature of police forces in the UK regarding major issues, everybody looks to everybody else to take a lead. The end result is that no one takes the lead.

12. I have written to all the Chief Constables and I have briefed a number of police forces who have been individually supportive of our solution. I have also briefed the Home Office on numerous occasions and I have supplied full information to ACPO and HMIC. But I firmly believe without a central lead from the Home Office very little can be achieved, and as a result, we are presently winding down our activity within the UK and concentrating abroad.

There is no doubt in my mind that one day soon this or similar technology will become vital to UK law enforcement, probably as the result of a further terrorist atrocity. What a pity that UK decision-makers appear only to react to something after the event.

Thank you for taking the time to consider my evidence. I remain at your disposal should you require any further information.

Robert Czapiewski
 Director
 ICT Cambridge Ltd

30 March 2006

5. Memorandum submitted by the Foundation for Information Policy Research (FIPR)

We were asked by the Committee to submit evidence on:

- the need to decrypt computer files;
- the length of time needed to obtain and analyse data from mobile phones; and
- problems in dealing with growing masses of digital forensic material.

We have been shown submissions by Assistant Commissioner Andy Hayman and by Peter Sommer. We should point out that Peter Sommer is also a member of FIPR’s Advisory Council and has been consulted on this response.

We would like to make the following points.

1. Modern cryptography tends to break quickly or not at all—either the data were encrypted using a bad product or a good one, and in the latter case you either guess the password or give up. Depending on the tools in use, it might take a few hours to a few days to try a large database of possible passwords on seized material; one tries out various dictionaries, girls’ names, names of Premiership footballers, etc. (There are one or two products that still use medium-strength cryptography, but they are becoming obsolete: and even in these cases, cryptanalysis is easy to parallelise, in that a key which takes a month to break on a PC can be broken in a day on 30 PCs if the matter is urgent.) Thus cryptography *per se* does not justify an extended pre-charge detention period.

2. Obtaining data such as call logs and location history from phone companies under the RIP Act should be a fairly rapid process, as the information is stored on automated systems and there are established procedures for law enforcement agencies to work through single points of contact with the companies. While there may occasionally be delays, there are now procedures for expedited access when a matter is urgent. There is thus no good reason why access to traffic and location data should justify an extended pre-charge detention period.

3. We are concerned, though, that by concentrating on low-level operational aspects such as performing cryptanalysis and getting data for traffic analysis, the police may be missing the larger strategic picture, as follows.

4. The amount of data available in trials, both civil and criminal, is increasing much more rapidly than the capabilities of police, prosecutors, defence lawyers, and even lawyers in civil cases. Investigators are trying to drink from a fire hose, and the volume is being turned up all the time.

5. For example, Operation Ore presented the UK police with a list of 7,000+ people who had bought pornography from a site in Texas that contained, *inter alia*, illegal images of child abuse. It also contained material that was merely tasteless. Much of Britain's computer forensic capability has been tied up for the last three years in searching through confiscated PCs, trying to determine which type of images their owners purchased. Often evidence could not be found, and in some of these cases suspects may have been bullied into accepting cautions for "incitement to distribute" to get the cases off the books. The recent headlines about teaching blacklists are just part of the fallout from that practice.

6. As another example, I am currently an expert witness in a civil matter in which the receiver of a failed company obtained a search order against a former director and seized ten PCs. Five months later, subsidiary litigation is underway about searching this material and the protocols for access. Civil litigation also results in huge volumes of data being obtained as part of the discovery process. A minor contract dispute can throw up 10,000 emails, while the US class action against tobacco companies generated over 10 million pages of documents. If the only way you can deal with that is to pay lawyers £200 an hour to read them, then litigation will become even more the preserve of the rich. One might draw a comparison with warfare, where the costs (and capabilities) of platforms such as combat aircraft have increased by orders of magnitude since World War 2.

7. This is not to decry the importance of digital evidence and intelligence. Indeed, it is the very usefulness of such material that has led police forces round the world to seize material in ever-increasing quantities, with the result that the existing analytic capacity is badly overstretched. Technological progress—the data storage equivalent of Moore's law—ensures that there will be ever-larger quantities of material to be seized. "Pervasive computing"—the process whereby processors and communications are embedded in ever more everyday devices, from TVs to cars—will ensure that ever more devices contain digital records that might potentially incriminate or exculpate a suspect. It is likely that within 5–10 years a search of a single home or small business will yield the thousands of gigabytes of data apparently encountered by the police in the wake of the July bombings.

8. New things can be done with digital evidence. For example, one can "undelete" files and email on seized computers, and perform rapid automatic searches for "known suspect" email addresses, phone numbers and even pornographic images.

9. However, neither the tools available to analyse this data, nor the UK police forces' capabilities in particular, have kept up with technology use by suspects.

10. Today's tools are designed to analyse a single hard drive at a time, using labour-intensive processes that do not scale well. They also do not usually support the kinds of analysis needed when a case involves large numbers of disk drives, such as correlation analyses to see which PCs were exchanging data with each other; recent academic research (Garfinkel) has shown the feasibility of such analyses. The task now is to design, build and deploy the tools.

11. FIPR has been concerned for years that UK police forces tend to devote less money, effort and priority to IT matters (such as computer crime and digital forensics) than would be socially optimal. This has also been the consistent (privately expressed) view of the most able practitioners within the system. A number of FIPR members have been involved in remediation activities ranging from police training to speaking at law-enforcement conferences.

12. In short, this is not a "terrorism" problem, but a general problem.

13. The solution is unlikely to be found in extended pre-charge detention, even for terrorist matters. In computer-science terms, the problem is not latency but bandwidth. In lay language: if the rate at which you seize PCs exceeds the rate at which you can image, index, search and analyse the contents, then the queue just keeps on getting longer. Extending time limits is at best a measure of desperation that gives only a one-off and very short period of respite. As data volumes double every 15 months, and as more and more devices acquire processors and communications, the solution cannot be found there.

14. FIPR believes that the police need a radical improvement in forensic capabilities: more experts, and better tools. The tools also need to be usable more widely, so that investigators are not stuck waiting for specialists. This is not just a resource issue, but an issue of attitudes and priorities at the policy level. IT must come out of the "ghetto"; a force that expects 90% of its officers to be able to drive and 30% to be qualified

in firearms should not be stuck with two computer-literate constables. Now that IT is part of the fabric of almost all our lives, the number of computer-trained officers should logically exceed the number trained in firearms and approach the proportion able to drive.

15. It must also be realised that sometimes information just will not be found, even when it is there. This already happens with non-digital evidence; from time to time a re-examination of old case material by a fresh mind or by new methods results in a conviction where none had been possible before, or even an acquittal on appeal of someone whose conviction was unsatisfactory or even mistaken.

16. The inevitable failures of digital evidence will include failures of new kinds. For example, complexity causes new problems. Much computer science and software engineering research over the past forty years has been directed towards developing tools and techniques to cope with ever-more complicated programs and data structures. An analogy we sometimes use is “climbing the complexity mountain”—with more and more effort one can get a little higher up, but the mountain always wins in the end. For example, it is often said that “one-third of large software projects fail”, and this seems as true now as in the 1960s. So has there been no progress in software engineering? On the contrary—we build much bigger and more expensive failures nowadays! The big project failures of the 1980s or even the 1990s might be quite manageable today. It is human nature to try to push the limits and achieve what no-one has done before, and the computer industry being young is less risk-averse than government.

17. Thus it should surprise no-one that the complexity of evidence available in some investigations and trials will exceed the analytic and management capabilities of the tools and techniques that the police have at the time. The existence of unmanageably complex cases cannot be accepted as a justification for extending the detention term, or we will end up with indefinite detention without trial.

18. Data retention is another issue that Parliament and the courts will have to tackle: should the police keep all data they have ever seen, as they have recently been doing with DNA data? There may be a case for this in terror and serious crime cases, but if data retention were to become universal for normal crime then police capabilities would be overloaded even worse than at present, and there would be serious conflicts with data protection and human rights law.

19. There are also matters of court procedure—in fact, quite fundamental issues of what it means to have a fair trial. As the quantity of material available to the prosecution and defence grows from the megabytes through the gigabytes into the terabytes and beyond, old-fashioned procedures for disclosure and discovery will become ever more inefficient and contentious. It will be increasingly easy for the prosecution to hide critical evidence in such a mass of irrelevant garbage that the defence are ambushed at trial. (I have been an expert witness in a civil matter where this happened.) Court procedure, in both criminal and civil sectors, has to be upgraded for the age of Google. This will raise many complex and difficult questions, and will no doubt have to be revisited every five to ten years as forensic and search technology both advance. I expect that such issues are beyond the remit of the committee’s present inquiry, and suggest that a separate inquiry might be a suitable way forward.

20. Fundamentally the question of how long it’s reasonable to keep people in jail from arrest to charge (and from charge to trial) is a political one. So is the question of what proportion of national resource is to be devoted to law enforcement and the legal system. Whatever time limits are imposed—from the wonderfully brisk 110-day rule in Scotland to the much more languid timescale considered normal in some foreign countries—police will work to these limits. Policemen, like everyone else, have conflicting claims on their resources; and if they have more time, they will take more time. They will also find cases in which (even with hard work) they cannot analyse the available data within the time limit or indeed at all. Arguments can always be made that given more time case X might have been solved. A sceptic will point out that the real limit is not usually the technology, but the attention and stamina of the human investigators. The point of diminishing returns is reached all too soon.

21. The computer industry’s response to the complexity inherent in large systems may provide an instructive parallel. Successful project management requires a rather brutal approach: the manager must focus hard, close down options, parallelise the work where possible and ship a good product within the time limit set by the customer. Investigators will have to learn these skills, and find appropriate ways to develop and exercise them within a framework that gives full access to the defence, and the benefit of the doubt to the accused.

22. It is also worth remembering that how long we keep people in jail is, at a deep level, a statement about what sort of society we believe we are, and what sort of society we collectively decide—through our elected representatives—to become.

23. In conclusion, FIPR does not believe there is a sound technological argument for increasing the detention time limits. There is a strong argument, however, for supporting the police in pushing through the necessary cultural change—and acquiring the necessary budgets—to get abreast of the opportunities that digital evidence provides.

Professor Ross Anderson
Chair, FIPR

27 January 2006

6. Memorandum submitted by JUSTICE

SUMMARY

1. Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance justice, human rights and the rule of law. It is also the British section of the International Commission of Jurists.

2. JUSTICE opposes the proposed increase in the maximum period of pre-charge detention for persons suspected of terrorism offences. It is important, though, to be clear about the nature of our opposition. We do not question that the current threat of terrorism is an extremely serious one. The attacks of 7 July have demonstrated this beyond doubt. Rather, we oppose extending the current maximum period beyond 14 days because we do not accept the argument—put forward by senior police officers and government officials—that the current limit is insufficient.

3. In this submission, we set out the reasons why we consider the existing limit to be sufficient. An important reason, though not the only one, is our view that 14 days is the maximum period likely to be held compatible with fundamental rights, short of seeking a further derogation from the European Convention on Human Rights (“ECHR”). This submission also sets out our criticisms of the reasons put forward by the Association of Chief Police Officers (“ACPO”) and others for extending the maximum period.

4. We note that increased judicial supervision of pre-charge detention has been suggested by some—including Lord Carlile of Berriew QC, the current statutory reviewer of anti-terrorism legislation—as a means of making longer periods of pre-charge detention compatible with the ECHR. We are critical of these proposals, together with the specious analogies that some have drawn with longer periods of post-charge detention in other European jurisdictions. As an organisation that seeks, among other things, to promote increased reference to international and comparative law in the development of UK law, we certainly do not oppose consideration of terrorist detention powers in other jurisdictions. But, in our view, the difficulties experienced by police and prosecutors in relation to counter-terrorism investigations would be better addressed by:

- greater attention to and, if necessary, further clarification of the Threshold Test in section 6 of the Code for Crown Prosecutors;
- bringing into force Part 3 of the Regulation of Investigatory Powers Act 2000; and
- lifting the long-standing ban on the admissibility of intercept evidence.

THE REQUIREMENTS OF ARTICLE 5(3) ECHR

5. Article 5(3) of the European Convention on Human Rights provides that anyone arrested on suspicion of a criminal offence:

shall be brought promptly before a judge or other officer authorised by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial.

6. In the 1988 decision of *Brogan v United Kingdom*,¹⁷ the European Court of Human Rights considered the case of three suspected IRA members who were detained under the Prevention of Terrorism Act (Temporary Provisions) Act 1984 for periods up to four days without being brought before a judge. The Court acknowledged that “the investigation of terrorist offences undoubtedly presents the authorities with special problems”,¹⁸ but concluded that:¹⁹

none of the applicants was either brought “promptly” before a judicial authority or released “promptly” following his arrest. The undoubted fact that the arrest and detention of the applicants were inspired by the legitimate aim of protecting the community as a whole from terrorism is not on its own sufficient to ensure compliance with the specific requirements of Article 5(3).

7. In *Brogan*, the Court made clear that “judicial control of detention” was one of the central guarantees of the right to be brought promptly before a court under Article 5(3):²⁰

Judicial control of interferences by the executive with the individual’s right to liberty is an essential feature of the guarantee embodied in Article 5(3), which is intended to minimise the risk of arbitrariness. Judicial control is implied by the rule of law, “one of the fundamental principles of a democratic society . . . , which is expressly referred to in the Preamble to the Convention” . . . and “from which the whole Convention draws its inspiration” . . .

¹⁷ EHRR 117. Compare the decision of *Brannigan and McBride v United Kingdom* (1994) 17 EHRR 539 in which similar periods of detention were held to be covered by the UK’s derogation following the *Brogan* decision.

¹⁸ *Ibid*, para 61.

¹⁹ *Ibid*, para 62.

²⁰ See eg *ibid*, para 58.

8. An essential feature of this “judicial control” under Article 5(3) is that the judge has the power to order the release of the suspect.²¹

9. The European Court of Human Rights has continued to make clear that those arrested or detained must be brought before a court “promptly”. As recently as 6 and 11 October 2005, the Court handed down two further judgments concerning detention periods during counter-terrorism investigations in South-Eastern Turkey.²² In both cases, the Court found that detention of more than six days in custody without being brought before a judge was a breach of Article 5(3), “notwithstanding the special features and difficulties of investigating terrorist offences”.²³

THE COMPATIBILITY OF THE EXISTING 14-DAY LIMIT WITH ARTICLE 5(3)

10. The current maximum of 14 days is set out in Schedule 8 to the Terrorism Act 2000 (as amended by section 306 of the Criminal Justice Act 2003). We note that the original maximum period set out in the Terrorism Act 2000, prior to its amendment in 2003, was seven days. The then-Home Secretary explained the purpose of the seven day maximum in the following exchange:²⁴

The Secretary of State for the Home Department (Mr. Jack Straw): The United Kingdom Government have had to enter a derogation from the [Human Rights Act 1998] because of the executive power for extensions of detention. That derogation arose from the case of *Brogan*, which came before the European Court. [. . .]

Mr. Kevin McNamara (Hull, North): When will my right hon. Friend inform the Council of Europe that the derogation from the Human Rights Act 1998 no longer needs to apply to Britain?

Mr. Straw: We should be able to do that when the Terrorism Bill becomes law.

11. Specifically, Schedule 8 introduced a degree of judicial control over detention by requiring judicial authorisation for any detention exceeding 48 hours. It was argued that this judicial involvement would be sufficient to meet the requirements of Article 5(3) in respect of pre-charge detention between two and seven days. The same argument was offered in respect of the increase in the maximum period from seven to 14 days in debates on the Criminal Justice Act 2003.²⁵

12. However, the compatibility of the provision—either as it was originally enacted nor as amended—has not been considered by the Strasbourg Court. Nor is it clear that the existing 14 day limit is necessarily compatible with the requirements of Article 5(3). For instance, paragraph 33(3) of Schedule 8 allows a judge considering an application for further detention to exclude the suspect and his lawyer from the hearing. Paragraph 34 similarly allows the judge to withhold disclosure of evidence relied upon by the police in support of an application for further detention. We strongly doubt whether these provisions would comply with the complementary requirements of Article 5(4) that a suspect have the benefit of the full judicial guarantees of a court, including disclosure of adverse evidence and the assistance of counsel. Whether or not these provisions would themselves be found compatible with Article 5(3), however, we strongly doubt that any pre-charge detention greater than 14 days authorised under the proposed amendments to the 2000 Act would meet its requirements.

POLICE AND GOVERNMENT ARGUMENTS FOR EXTENDING MAXIMUM PERIODS OF PRE-CHARGE DETENTION

13. In a note annexed to the Terrorism Bill when it was published in draft on 15 September,²⁶ the government advanced a number of justifications for seeking longer detention periods in criminal cases, including:

- the nature of the terrorist threat, ie the need to intervene early in order to prevent a possible attack;
- difficulties in decrypting heavily-encrypted computer data;
- the large volume of evidence in criminal cases;
- complexity of terrorist networks;
- international nature of terrorism, including the need to use interpreters;
- delays involving the handling of CRBN and other hazardous substances;
- other difficulties in recovering of evidence from a crime scene; and

²¹ See *Schiesser v Switzerland* (1979) 2 EHRR 417, para 31: Art 5(3) imposes on judges “obligations of reviewing the circumstances militating for or against detention, of deciding, by reference to legal criteria, whether there are reasons to justify detention and of ordering release if there are no such reasons”.

²² *Sinan Tanrikulu and others v Turkey* (application nos 00029918/96, 00029919/96 and 00030169/96, 6 October 2005); *Yasar Bazancir and others v Turkey*, (application nos 00056002/00 and 0007059/02, 11 October 2005).

²³ *Tanrikulu*, *ibid*, para 41.

²⁴ *Hansard*, HC Debates, 15 March 2000, Col 474. See also the explanation of the Home Office Minister Lord Bassam of Brighton, HL Debates, 6 April 2000, Col 1432: “In order to withdraw those derogations the Bill provides a system for extensions of detention under independent judicial authority. The Government intend to lift their derogations once those provisions are in force”.

²⁵ See eg Baroness Scotland of Asthal, *Hansard*, HL Debates, 15 October 2003, Cols 961–962.

²⁶ Annex A, *Pre-Charge Detention Periods*, 15 September 2005.

- delays caused by religious observance and the use of a single solicitor by suspects.

14. We note, however, that many of these arguments are not new, having been considered and rejected before. Indeed, it is striking to compare the arguments put forward by the government during the debates on the current Bill with those that it advanced in the *Brogan* case before the European Court of Human Rights:²⁷

The Government have argued that in view of the nature and extent of the terrorist threat and the resulting problems in obtaining evidence sufficient to bring charges, the maximum statutory period of detention of seven days was an indispensable part of the effort to combat that threat, as successive parliamentary debates and reviews of the legislation had confirmed . . . In particular, they drew attention to the difficulty faced by the security forces in obtaining evidence which is both admissible and usable in consequence of training in anti-interrogation techniques adopted by those involved in terrorism. Time was also needed to undertake necessary scientific examinations, to correlate information from other detainees and to liaise with other security forces.

15. Similarly, difficulties in decrypting heavily-encrypted computer data were cited by the government in supporting the 2003 extension of pre-charge detention from seven to 14 days:²⁸

A further layer of complexity that technological development has added is that investigations increasingly involve the requisition and analysis of hard drives of PCs and the subsequent search of suspects' work or home premises after an arrest has been made. It is therefore a matter of days, not hours, before any material from a hard drive is available to be used in the questioning of a suspect. This can be further exacerbated when the hard drives or PCs obtained from a number of individuals have to be cross-referenced to each other to establish patterns of communication and even movement.

16. While we do not doubt that police face difficulties in carrying out terrorism investigations, we are sceptical of the same arguments being deployed to justify ever-increasing periods of pre-charge detention. In respect of the encryption argument, for instance, we note that the government has yet to bring into force the powers under Part 3 of the Regulation of Investigatory Powers Act 2000 to require a suspect to provide an encryption key. We find the government's failure to do so particularly surprising given that it is prepared to cite difficulties in de-encrypting computer files as a justification for significantly extending pre-charge detention.

17. Investigative difficulties notwithstanding, the government and police have been unable to point to a single case in which a suspect was held for the existing maximum period of 14 days and then released without charge. Were the existing limit as inadequate as has been claimed, one would expect to find several cases in which suspects had been held for 14 days and then released. The absence of such cases supports our view that the existing 14-day limit provides police and prosecutors with sufficient time in which to charge terrorism suspects. In support of this view, we also note the following.

18. First, it is well-established that the police may only arrest a person where they have reasonable suspicion that the person has committed a criminal offence.²⁹ This means that there must already be some grounds for their belief and, thus, some evidence to support a charge under one or more criminal offences.

19. Secondly, the existing range of terrorist offences is extremely broad and the range of non-terrorist criminal offences even broader. We therefore consider it most unlikely that the police and Crown Prosecution Service will take more than two weeks at the maximum to identify an appropriate charge that would enable the suspect to be brought before a competent court and an application for bail considered.

20. Thirdly, we note that section 6 of the Code for Crown Prosecutors provides a "Threshold Test" for those cases in which:³⁰

it would not be appropriate to release a suspect on bail after charge, but the evidence to apply the Full Code Test is not yet available.

[. . .] There will be cases where the suspect in custody presents a substantial bail risk if released, but much of the evidence may not be available at the time the charging decision has to be made. Crown Prosecutors will apply the Threshold Test to such cases for a limited period.

21. The Threshold Test allows a Crown Prosecutor to have regard to:³¹

- the evidence available at the time;
- the likelihood and nature of further evidence being obtained;
- the reasonableness for believing that evidence will become available;
- the time it will take to gather that evidence and the steps being taken to do so;
- the impact the expected evidence will have on the case; and

²⁷ *Brogan*, n1 above, para 56.

²⁸ *Hansard*, HL Debates, Baroness Scotland of Asthal, 15 October 2003, Col 964.

²⁹ Section 24 of the Police and Criminal Evidence Act 1984, as amended by section 110 of the Serious Organised Crime and Police Act 2005.

³⁰ Sections 6.2 and 6.3.

³¹ Section 6.4.

— the charges that the evidence will support.

22. Most significantly, the Threshold Test is expressed in terms of “reasonable suspicion”, ie the same standard that the police employ in deciding whether a suspect should be arrested.³²

The Threshold Test requires Crown Prosecutors to decide whether there is at least a reasonable suspicion that the suspect has committed an offence, and if there is, whether it is in the public interest to charge that suspect.

23. In the circumstances, we consider that if there were sufficient evidence to support reasonable suspicion on the part of the police arresting an individual on suspicion of one or more terrorism offences, there would be no difficulty in satisfying the Threshold Test as set out above.

24. Fourthly, we note that section 16.5 of Code C of the Police and Criminal Evidence Act 1984 allows for the questioning of a suspect post-charge if it is necessary to “prevent or minimise harm or loss to some other person, or the public”.³³

25. Fifthly, we note that much of the discussion concerning pre-charge detention in the UK has been hopelessly flawed by inaccurate comparisons with post-charge detention in a number of European jurisdictions. According to the comparative study recently released by the Foreign and Commonwealth Office,³⁴ none of the European jurisdictions surveyed appeared to allow pre-charge detention longer than six days:

- France four days;³⁵
- Germany two days;³⁶
- Greece six days;³⁷
- Norway two days;³⁸
- Spain five days.³⁹

26. Although it is correct that several European countries allow for extensive periods of detention post-charge, it is also possible to be detained post-charge in the UK, ie where a suspect is refused bail. More generally, we are concerned at suggestions that extensive periods of pre-charge detention could be justified by incorporating a degree of judicial control along the lines of some of the above European jurisdictions. The role of examining magistrates in such civil law jurisdictions as France is vastly different to that in common law countries such as the UK.⁴⁰ In particular, the role of the examining magistrate is not merely to provide an independent check upon criminal investigation by the police but to actively direct that investigation. This indicates a degree of judicial control over criminal investigations far in excess of that found in any common law jurisdiction based on an adversarial—rather than inquisitorial—system of justice. We therefore caution strongly against seeking to import features from other systems of law without first understanding the very different distribution of checks and balances in those systems.

27. Finally, we note that much of the justification for extending the period of pre-charge detention is premised on the situation where the reasonable suspicion for arrest is based on evidence that is inadmissible at trial, eg intercept evidence. We have long argued⁴¹ that the ban on the admissibility of intercept evidence should be lifted, and our conclusion was supported by the recommendations of the Newton Committee in 2003.⁴² As the author of the 1996 review of counter-terrorism legislation,⁴³ the former Law Lord Lord Lloyd of Berwick, noted during parliamentary debate on the Regulation of Investigatory Powers Bill in 2000:⁴⁴

We have here a valuable source of evidence to convict criminals. It is especially valuable for convicting terrorist offenders because in cases involving terrorist crime it is very difficult to get any other evidence which can be adduced in court, for reasons with which we are all familiar. We know who the terrorists are, but we exclude the only evidence which has any chance of getting them convicted; and we are the only country in the world to do so.

³² Section 6.1, emphasis added.

³³ Police and Criminal Evidence Act 1984, Code C, section 16.5: “A detainee may not be interviewed about an offence after they have been charged with, or informed they may be prosecuted for it, unless the interview is necessary: to prevent or minimise harm or loss to some other person, or the public”.

³⁴ Foreign and Commonwealth Office, *Counter-Terrorism Legislation and Practice: A Survey of Selected Countries* (October 2005).

³⁵ *Ibid*, para 32.

³⁶ *Ibid*, para 40.

³⁷ *Ibid*, paras 54–55.

³⁸ *Ibid*, para 84.

³⁹ *Ibid*, para 94.

⁴⁰ While Scottish law is on civil law principles, the role of the judge in criminal proceedings in Scotland appears far closer to that in England, Wales and Northern Ireland than to other civil law jurisdictions.

⁴¹ JUSTICE, *Under Surveillance: Covert Policing and Human Rights Standards*, p 76: “there is a growing consensus that [the] restriction is now unsatisfactory and that material lawfully obtained through an interception should be *prima facie* admissible evidence, subject to the usual judicial discretion under section 78 [of the Police and Criminal Evidence Act 1984] on fairness grounds”.

⁴² Privy Counsellors Review Committee, *Anti-Terrorism Crime and Security Act 2001 Review: Report* (HC100: 18 December 2003), para 208.

⁴³ Lord Lloyd of Berwick, *Inquiry into Legislation against Terrorism*, 30 October 1996 (Cm 3420). The report identified at least 20 cases in which the use of intercept evidence would have allowed a prosecution to be brought—see vol 1, p 35.

⁴⁴ See *Hansard*, HL Debates, 19 June 2000, Col 109–110. Emphasis added.

28. Lifting the ban on admitting intercept evidence would bring UK criminal procedure into line with that of the great majority of common law jurisdictions, including Canada, Australia, South Africa, New Zealand and the United States.⁴⁵ If the use of intercept evidence is admissible on a regular basis in these other jurisdictions, it seems difficult to conceive of a compelling reason for the government to maintain the current self-imposed ban while at the same time seeking to justify a departure from basic standards of fairness in other areas.

ESTABLISHING A JUDICIAL ROLE IN THE INVESTIGATION OF TERRORIST OFFENCES

29. We are aware that there is support in some quarters for increased judicial involvement in the investigation of terrorist offences. In this context we note the recommendations of the Newton Committee in 2004 and the more recent support given by Lord Carlile of Berriew QC to increased judicial involvement in the pre-charge detention process in the debate over the Terrorism Bill.⁴⁶

30. The Newton Committee recommended, among other things, the possible use of security-cleared judges to assess evidence on a more inquisitorial basis.⁴⁷ This, it was suggested at the time, might be a way to increase the likelihood of criminal prosecutions for terrorist offences in view of the significant evidential hurdles that the Committee had identified. While we agreed with the Newton Committee's call for a more structured system of disclosure of evidence,⁴⁸ it was at the time wholly unclear to us how the Committee foresaw the use of security-cleared judges screening evidence⁴⁹ might improve on the admissibility of material from the current system. It was particularly unclear what weight the "fair answerable case" assembled by one judge would have in full criminal proceedings before another, particularly if the preliminary hearing were conducted on an inquisitorial rather than adversarial basis. The findings of a judge (particularly one who has seen evidence not disclosed at trial) would likely to carry great weight with a subsequent judge and jury, and would effectively preempt much of what ought properly to be determined in-trial. The unfairness of determining guilt or innocence, be it by a judge or jury, on evidence that is not disclosed to an accused and upon which he or she cannot make comment or challenge should be manifest and is likely to breach the right in Article 6(3)(d) ECHR to "examine or have examined witnesses against him".

31. We are equally sceptical of the recent suggestions made by Lord Carlile, the Independent Reviewer of Terrorism legislation, in respect of increased judicial involvement in the pre-charge detention process. We agree with his analysis that district judges would not be suited to the task of considering applications for longer periods of detention than the current two-week maximum.⁵⁰

A more searching system is required to reflect the seriousness of the State holding someone in high-security custody without charge for as long as three months.

However, the specific proposals that Lord Carlile then puts forth to provide a "reassuringly strong system of protection for the detained person" seem to us to fall far short of that goal. First, he proposes "the introduction of one of a small group of security-cleared, designated senior circuit judges as examining judge".⁵¹ We note, however, that those civil law jurisdictions such as France that employ examining magistrates and inquisitorial methods provide far more specific and intensive training for the task of supervising (and, indeed, directing) criminal investigations than does the common law system. Lord Carlile makes reference to his proposals comparing favourably to those available in the United States (the only common law jurisdiction he cites as a comparison)⁵² and yet we are unaware of any comparable provision for pre-charge detention in US state or federal law.

32. Secondly, Lord Carlile proposes the introduction of a "security-cleared special advocate . . . to make representations on the interests of the detained persons and to advise the judge".⁵³ However, Lord Carlile nowhere explains how such a system (hitherto used only in civil proceedings and in public interest immunity applications in criminal proceedings) would be compatible with the guarantees of Articles 5(4), which include the right to full disclosure of adverse material. The idea that a suspect could be detained for what Lord Carlile acknowledges to be lengthy periods of time without knowing the full case against him or her seems to us to be antithetical to basic notions of fairness. As Lord Steyn noted in his dissenting judgment in *Roberts v Parole Board*:⁵⁴

It is not to the point to say that the special advocate procedure is "better than nothing". Taken as a whole, the procedure completely lacks the essential characteristics of a fair hearing. It is

⁴⁵ See Lord Lloyd, *ibid*, col 106: "evidence of telephone communications of that kind is admissible in court in every country in the world as I am aware. The countries I visited during my inquiry into terrorism—France, Germany, the United States and Canada—regard such evidence as indispensable. They were astonished to hear that we do not use it in this country".

⁴⁶ *Proposals By Her Majesty's Government For Changes To The Laws Against Terrorism*, 12 October 2005.

⁴⁷ *Newton Report*, paras 224, 228.

⁴⁸ *Newton Report*, paras 236–239.

⁴⁹ *Ibid*, para 231: "An investigative approach would address the disclosure problem by putting a security-cleared judge in control of assembling a fair, answerable case".

⁵⁰ See n44 above, para 64.

⁵¹ *Ibid*, para 67.

⁵² *Ibid*, para 68.

⁵³ *Ibid*, para 67.

⁵⁴ [2005] UKHL 45 at para 88.

important not to pussyfoot about such a fundamental matter: the special advocate procedure undermines the very essence of elementary justice. It involves a phantom hearing only.

33. Thirdly and more generally, little thought appears to have been given for the longer-term consequences of seeking to introduce inquisitorial methods of justice into the common law system of adversarial justice. It is sufficient to note that much of what is originally presented as wholly exceptional, once introduced, becomes part of the general fabric of the law: the process variously known as “legislative creep” or “function creep”. For the arguments from complexity that are made in the context of terrorism offences are equally applicable to serious organised crime and serious fraud. From there, it would not be too difficult for a government to subsequently argue that—since the process is already in place for serious criminal offences—consistency demands that the same procedures should be applied to ordinary criminal prosecutions as well. It is perhaps sufficient to notice how the stop and search powers of section 44 of the Terrorism Act 2000, originally introduced to fight terrorism, appear to have become part of the general array of police powers.⁵⁵

34. It is worth noting that many of the above arguments were first put forward by the UK government when it argued against further judicial involvement in pre-charge detention before the European Court of Human Rights in *Brogan*.⁵⁶

As regards the suggestion that extensions of detention beyond the initial 48-hour period should be controlled or even authorised by a judge, the Government pointed out the difficulty, in view of the acute sensitivity of some of the information on which the suspicion was based, of producing it in court. Not only would the court have to sit in camera but neither the detained person nor his legal advisers could be present or told any of the details. This would require a fundamental and undesirable change in the law and procedure of the United Kingdom under which an individual who is deprived of his liberty is entitled to be represented by his legal advisers at any proceedings before a court relating to his detention. If entrusted with the power to grant extensions of detention, the judges would be seen to be exercising an executive rather than a judicial function. It would add nothing to the safeguards against abuse which the present arrangements are designed to achieve and could lead to unanswerable criticism of the judiciary.

35. We continue to support the Newton Committee’s call for a more structured system of disclosure of evidence. There is also perhaps a greater role for judges to play in facilitating increased use of sensitive intelligence material in criminal proceedings. However, we strongly oppose any extension of pre-charge detention beyond the current maximum of two weeks and we harbour serious doubts whether any suitable procedures of “judicial control” could be devised under our existing adversarial system of justice that would be sufficient to safeguard fundamental rights. To compare the role of a judge from a common law system with that of an examining magistrate in a civil law jurisdiction fails to compare like with like. We therefore caution strongly against importing features from other systems of law without at least understanding the different distribution of checks and balances in those systems, not to mention the careful equilibrium of our own.

Eric Metcalfe
 Director of Human Rights Policy
 12 December 2005

7. Memorandum submitted by David Lattimore

This report is in response to the Committee’s notice of 25 November 2005. Its purpose is to promote the understanding of Computer forensics, encryptions and the investigative process thereof.

1. INTRODUCTION

This report has been produced from a computer forensic practitioner’s perspective, to promote the understanding of computer forensics, encrypted data, the subsequent analysis & the investigative process. Its purpose is to assist the Committee with reference to Terrorism Detention Powers.

2. QUALIFICATIONS AND EXPERIENCE

I am the Technical Manager of the Digital Crime Unit LGC and specialise in the examination of computer and digital media equipment for forensic purposes. I have been involved in this type of work since 1992. A profile is attached and a full CV has been submitted [*not printed*].

⁵⁵ See eg BBC Online, “*Hero’s return for Labour heckler*”, 29 September 2005.

⁵⁶ n1 *ibid*, para 56.

3. FORENSIC PROCEDURES

The forensic examination of computer hard-disks has developed significantly over the last 13 years. In the early days, law enforcement agencies developed procedures in order to comply with the rules of evidence. In 1998 the Good Practice Guide published by the Association of Chief Police Officers (ACPO) laid down the principles relating to the forensic examination of computers and digital media. Today these standards are not only used by law enforcement agencies but also by many commercial and independent computer forensic investigators.

4. COMPUTER HARDWARE TECHNOLOGY

Computers have developed over the last 15 years at an alarming rate especially hard-disk sizes. In the early days computers investigated by law enforcement agencies normally contained only one small hard-disk. Today it's not unusual to find computers with two or three hard-disks of a vast size. Also with the cheapness of computer hardware it's not unusual to find users with more than one computer, laptops, removable hard drives, USB memory devices, digital cameras, GPS devices and vast amounts of writable CD ROM's and DVD's all of which require forensic examining. It's not unusual for an investigator to be tasked to deal with a large amount of data storage per suspect.

5. FORENSIC IMAGING

The forensic investigator having received a computer will, after initial physical examination, remove the hard disk(s) for imaging. This is the process where an exact copy of the hard drive is made with forensic tools. One of the main reasons for this is that a forensic examination will be made of the hard disk image itself and not of the original hard disk. This reduces the possibility of an allegation that the data evidence has been contaminated. It also allows the defence to receive an exact copy of the hard disk to view or dispute the evidence found. Imaging times can vary from less than an hour to many hours depending on the size of the hard-disk; often the process is allowed to proceed overnight. Some forensic software allows for the previewing of hard drives without imaging, however from experience although this might be satisfactory for initial indication, certain data such as encrypted data and steganography, can be missed. Normally the forensic investigator who has previewed a hard drive would go on to make a complete image and carry out a thorough examination.

6. THE FORENSIC ANALYSIS

The forensic examination can vary in the length of time it takes depending on the size and the content of the hard drive. A large hard drive with little data and few user files may only take a short period of time. However a small hard drive that is populated with 100,000s of files and programs and data in slack and unallocated space will take considerably longer. If I had to put a time on the forensic analysis of an average hard drive, say 80GB, then I would normally take between three to five days. If a suspect has taken specific steps to hide or remove data a more in depth analysis will be required which will take longer.

7. ENCRYPTION ISSUES—A BRIEF OVERVIEW

Data can be encrypted in a number of ways. Individual files or a volume which holds many files can be encrypted and stored on any data holding device alternatively whole hard drives can be encrypted.

There are many programs available to users to encrypt data on computers. These are available either from the Internet (often free), computer magazines or are passed on by associates. The strength of encryption varies with the program used. This strength depends on two key factors, the type of encryption used (known as the algorithm) and the length of the key used. There are two main types of encryption symmetric and asymmetric.

Symmetric encryption requires that the same key, or password, be provided to all those who require access to the encrypted file. The key is the same for everyone. The weakness with this type of encryption is that an investigator can determine the key or with a powerful computer discover the password. Some can take a few seconds to discover and some can take many years.

Asymmetric encryption requires the use of two keys: a public key and a corresponding private key. When a file is encrypted, the public key of the recipient is used to encrypt the file. The recipient provides the public key to the creator of the encrypted file. The only key that will decipher the file is the private key that is known only by the recipient. It's not unusual for a user of this type of encryption to remove the private key from the computer the encrypted file is on. The private key can be stored at a remote location on the internet, or on removable devices such as USB memory sticks and other computers. Despite its strength, it can still be possible to crack an asymmetric cipher using a brute force attack.

Steganography is not actually a method of encrypting messages, but is a way of hiding data within something else, such as a graphic or sound file, to enable the data to be undetected. It has been known for suspects to encrypt the file using asymmetric encryption then use steganography to hide it further before sending it via an e-mail.

During the forensic examination an investigator should determine whether any encrypted files, volumes or encryption programs exist on the hard drive. Often some encrypted files/volumes are found however others are missed because the investigator is not familiar with the techniques being used by the suspects.

8. CRACKING ENCRYPTED FILES & VOLUMES

The strength of the encryption used varies with the algorithm from 40 bit up to 2,048 bit. 40 and 56 bit algorithms are weak encryption. 40 bit will give one trillion (1,097,728,000,000) possible key combinations and 56 bit will give almost 72 thousand quadrillion (71,892,000,000,000,000) possible key combinations.

Although this type of encryption is often used it is more common to use a stronger algorithm such as 128 bit which will give = 339,000,000,000,000,000,000,000,000,000,000,000,000,000 (give or take a couple of trillion) possible key combinations.

Cracking a 56 bit algorithm using one computer testing 1,000,000 keys per second could take up to 2,284,931 years. The same algorithm using 2000 computers could take up to 1.1 years.

Cracking a 128 bit algorithm using one computer testing 1,000,000 keys per second could take up to 10,790,283,070,806,000,000,000,000,000 years. The same algorithm using 2,000 computers could take up to 5,395,141,535,403,010,000,000,000 years.

Therefore it's not always practical to decrypt the encrypted file/volume by a brute force attack although it is possible.

If a brute force approach is taken the forensic analyst may need to develop a specific "crack" for the particular encryption, if one has not been previously developed. The "crack" enables the brute force attack to commence.

9. BIOGRAPHICAL PROFILING

10. THE FUTURE

New and stronger algorithms are being developed and will be freely available through various sources. The biggest problem forensic analysts will face in 2006 is the release of Microsoft new operating system called "Vista". This is due for release in September or October.

One of the main features of Microsoft Vista is its enhanced security facility "Bit Locker" which used to be called "Full Volume Encryption".

In brief "Bit Locker" will apply full hard drive encryption all the time. To decrypt the hard drive a "Startup key" will be required to log on to the computer. A startup key can either be physical (USB flash drive with a machine-readable key written to it) or personal (a PIN set by the user). The user inserts a USB Flash Drive key in the computer before turning it on. The key stored on the flash drive unlocks the computer. Without this key the data will not be accessible. The reason for this is physical security which prevents a thief who steals the PC or Laptop and then removes the hard drive from accessing its contents. What forensic analysts do to image the hard drive is to remove it from the computer to prevent anything being written to it. Therefore this facility will create problems for forensic analysis.

The mobile phone will become more like a computer with the introduction of mini hard disks creating new challenges for the forensic analyst.

Computers and data devices hold a wealth of intelligence which is not exploited enough by law enforcement agencies. Recently whilst at LGC a fraud case I was working on revealed data linked to the Middle East and certain terrorist groups. As a result this data was supplied separately to the Special Branch of the Police Force who submitted the computer for analysis. It proved so valuable that the data is now with the security services for further investigation. Law enforcement agencies must consider the intelligence available from the data devices seized.

11. CONCLUSION

This report has provided a very brief overview of Computer Forensics and encryption. It is evident that technology will continue to grow and the use of strong encryption will become more widespread amongst criminals as well as everyone else. The use of facilities such as the National Technical Assistance Centre (NTAC) by law enforcement agencies will be paramount in dealing with encrypted files and volumes. However forensic analysts must be trained to identify when encryption of any sort is present on data devices.

Dealing with data on the many devices that are now seized by law enforcement agencies is a very time consuming job. If the forensic analysis is rushed relevant data can be missed.

In my experience the only way to deal with encryption found on data devices is by way of Biographical Profiling which as stated earlier is a time consuming exercise.

I would be happy to expand on the points covered in this report if required to do so.

12. GLOSSARY OF TERMS

Bit

A bit refers to a digit in the binary numeral system. A byte is a collection of bits, originally variable in size but now almost always eight bits.

Brute Force Attack

In crypto-analysis, a brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys in order to decrypt a message. In most schemes, the theoretical possibility of a brute force attack is recognized, but it is set up in such a way that it would be computationally infeasible to carry out. Accordingly, one definition of “breaking” a cryptographic scheme is to find a method faster than a brute force attack.

Hard Disk Drives and “Unallocated space”

The computer stores data electronically in a storage device called a hard disc drive. This hard disc drive can be of a varying size, but is now more commonly in the region of 80–200 Gigabytes in size. This is very large, and vast amounts of data can be stored on the disc itself. As a guide, a compact disc (CD) can store just over one half of a gigabyte (0.5 GB or 500 MB) worth of data alone. When software, such as operating systems (Windows 2000) and word processor packages (Microsoft Office) are installed onto the hard disc, the data will take up the space it needs to install and be able to run. This space can then be called “allocated”. Therefore, the unallocated file space relates to the space remaining on the hard disc that has not been used. However, if a file is deleted and deleted again from the “Recycle Bin” it is no longer accessible via the Windows operating system. The file itself has not been removed from the hard disc, it simply cannot be seen. It will remain on the hard drive unless the space it occupies is needed for re-use by the system. The file or the data from that file can be found using forensic recovery software, but the file itself is “said” to have been found in the “unallocated” file space.

Key

A key is a piece of information that controls the operation of a cryptography algorithm.

Slack space

Slack Space is the unused space on a hard disk between the end of a file and the end of the cluster that the file occupies. For example, on a drive with a 16 kb cluster size, there will be 5 kb of slack space at the end of an 11 kb file. The slack space is wasted, as it cannot be used by the computer for another file. This slack space can contain relevant data from previous deleted files.

Volume

An area on the hard drive that has been formatted so that files can be stored within it. A hard drive may contain a single or multiple volumes. Each volume appears as if it is a single hard drive. In Windows, the first volume is normally referred to as “C:” while subsequent letters, such as “D:”, “E:” etc, may refer to additional volumes or may identify devices such as a CD-ROM drive.

13. PROFILE

David Lattimore

I am a Technical Manager of the Digital Crime Unit of LGC specialising in the forensic analysis of computers, digital cameras, removable media and personal digital assistants (PDA’s) for evidential data.

A full CV has been submitted [*not printed*].

26 January 2006

8. Memorandum submitted by Liberty

ABOUT LIBERTY

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

LIBERTY POLICY

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent funded research.

Liberty's policy papers are available at

www.liberty-human-rights.org.uk/resources/policy-papers/index.shtml

INTRODUCTION

1. Liberty welcomes the opportunity to offer further comment on the proposed extension to pre-charge detention time limits. Our position throughout debate on the Terrorism Bill has been to avoid making comment on the compatibility with any specific extension with the European Convention on Human Rights (ECHR). The legality of pre-charge detention is governed by Article 5(3) of the ECHR. This provides that anyone arrested or detained must be brought before a judge within a reasonable time and tried or bailed. We have little doubt that the original 90 day period would have breached the Convention. However, to determine any argument over detention simply in the context of what detention period might be permissible would necessitate predicting what extension (if any) might be justified. Instead we have focused on the justification for extension put forward by the police and suggested that other, more proportionate alternatives should be considered before any extension could be justified. We are extremely pleased to see the Committee are asking for further evidence on the suggestion we have put forward.

ARGUMENTS FOR EXTENSION

2. Justifications for extension to pre-charge limits are set out in the letter sent by Assistant Commissioner Hayman to the Home Secretary on 6 October 2005. Before covering these we would re-iterate two points made in our original parliamentary briefing. First, other types of criminal investigation have similar problems as the type referred to in Assistant Commissioner Hayman's letter. For example, white collar fraud can involve huge amounts of material and any number of jurisdictions. Yet pre-trial detention is limited to a maximum of four days, less than a third of the current time permitted for terrorism detention. Second, unless there has been an attack or attempted attack which the police and security services were not aware of⁵⁷ arrests are likely to follow months of investigation and surveillance. The difficulties described in the AC's letter seem to imply that the arrest will be from a "standing start". In reality, it is difficult to see how months of investigation could not mean that there was a considerable amount of evidence available at the time of arrest. The crucial point to be made when considering detention time limits is that detention is the time allowed in order to gather sufficient evidence to bridge the gap between what is needed to arrest and what is needed to charge. This is not a large gap.

3. This second point is countered by Andy Hayman in his letter when he differentiates the threat of terrorism today from earlier Irish terrorism by saying that "Public safety demands earlier intervention. And so the period of evidence gathering that used to take place pre-arrest is now denied to the investigators". However, the earlier distinction drawn in the letter is based on the fact that "Irish Terrorists deliberately sought to restrict casualties for political reasons". This is a distinction of scale. The Irish terrorism campaign did result in a series of bombings causing multiple fatalities. The letter seems to suggest that need for earlier intervention and arrest during the Irish campaign would not have been as urgent at the present as the likely number of fatalities would have been fewer than the London bombings in July. It cannot be Assistant Commissioner Hayman's intention to argue that the number of likely casualties would be a relevant factor in deciding whether to intervene early.

4. The Committee has asked for comment on a number of specific points which we will address in turn. The international nature of terrorism is the first justification. We appreciate this could present problems but as indicated earlier other types of offending, such as international fraud, cover multiple jurisdictions and can involve incredibly complex evidence. Indeed it is the nature of complex fraud that evidence is likely to be extremely well hidden by those who may have perpetrated an offence. However, the permitted detention period for fraud is a maximum four days. Similar arguments can be made in relation to the argument that time is needed to decrypt computer files. As explained later on there are also powers available to require an individual to hand over encryption keys including a specific criminal offence under the Regulation of

⁵⁷ In which case we imagine there would be a considerable amount of evidence.

Investigatory Powers Act 2000. The government has countered by saying that people under arrest may not have access to encryption keys so these powers would not always help. This may be true. However, it seems likely that if the police have obtained sufficient evidence to arrest then it would be on the basis of information already gained from de-encrypted data from other computers. Once arrested it seems likely that they would hold encryption keys to any computer in their possession. Assistant Commissioner Hayman's letter uses similar arguments in relation to mobile phones. Powers to require retention of, and covering police access to, communication data are already considerable.⁵⁸ We imagine that communications data is of greatest use pre arrest as an intelligence and surveillance tool.

5. We do not see how difficulties in establishing identities of terrorist suspects would present any significant hindrance. Multiple identities are not a new phenomenon in criminal investigation. People can be charged under an identity they have assumed if that is a name by which they are known. Further investigation might establish an identity to be false but this would not prevent charge. It is difficult to imagine any situation, especially if it follows any period of surveillance and investigation, where a suspect was not known by any identity.

6. A lack of interpreters is also cited as a justification for extension. Anyone arrested will either be a UK or EU/non EU national.⁵⁹ Any non British national arrested on suspicion of terrorism is likely to be detained in any event as we presume the Home Secretary would determine that their presence is non conducive to the public good. A UK national is likely to speak English. If they do not then it is difficult to imagine a situation where they do not speak at least one relatively commonly spoken national language. Difficulties in obtaining interpreters demonstrate why it is important that the goodwill of differing racial and religious groups within the UK is vital. Liberty has expressed concerns on numerous occasions that the some of the legislative and policy excesses in anti terrorism policy will proved counterproductive as they will alienate sections of society.

7. The need for time for forensic analysis would appear to be one of the more persuasive arguments justifying detention extension. However, it is quite common in criminal cases for the majority of forensic evidence to be accumulated post charge as it will often take weeks of analysis. We imagine forensic evidence is likely to be one of several sources of evidence in terrorism cases. Even in situations where the only evidence is based on forensic analysis (such as when suspected drugs are sent for assessment) it is common to bail suspects back to the police station. As we explain later, this might be coupled with powers similar to those used in the Control Order regime under the Prevention of Terrorism Act 2005.

8. The last two justifications relate to detention conditions. We do not believe the need for religious observance should create any significant problem. The need to pray should not have any particular impact as the Police and Criminal Evidence Act 1984 (PACE) specifies the need for regular breaks anyway. Similarly delays arising from the same firm. Any delays caused by solicitors acting for several clients are unlikely to be overly problematic as more than one representative from a firm is likely to be involved in taking instructions. We note that there do not seem to have been any suggestions of a more proportionate approach if there is indeed a problem here. One thing that might be considered is to look at PACE code rules about interview timings to consider whether detainees who insist on speaking to a particular solicitor to the exclusion of others might have the "clock stopped" for a period if that representative is temporarily unavailable. We are hesitant to suggest this as a possibility as there would be considerable potential for abuse. We therefore mention it here in the spirit of offering more proportionate alternatives as requested by the Committee and raise it simply as a matter for consideration. We would also re-emphasise that terrorism suspects can already be delayed far longer than normally permitted and do not accept that having to wait for a few hours in itself justifies any extension.

ALTERNATIVES

9. Liberty has publicly stated on many occasions that we believe that the most effective way of combating terrorism is to ensure that the police and security services have the appropriate resources and powers to investigate and deal with those who are planning terrorist acts. Many of the justifications for increasing the pre-charge detention limits referred to in Andy Hayman's letter can be attributed to a lack of resources. One area of huge public spending in the coming years will be the Government's ID card scheme. It is estimated that the cost of introducing ID cards could cost anywhere between £6 billion (the Government's estimate) to £18 billion (the estimate given by the LSE in a study carried out in June 2005). Whatever the final cost, Liberty believes that the money would be better spent directly on police and security services resources. It is hard to see how an ID card could help with intelligence gathering against suspected terrorists. It is safe to assume that British intelligence agencies have gathered information on anyone that they believe could constitute a risk to national security. We cannot imagine what information held on the National Identity Register would add to that possessed by the Security Services. For the vast majority of people who are not involved in terrorist activity, their entry is irrelevant in combating terrorism.

⁵⁸ Covered by Part 11 Anti Terrorism Crime and Security Act and Part 1 Chapter 2 of the Regulation of Investigatory Powers Act respectively.

⁵⁹ Powers to deport EU nationals who are suspected of involvement in terrorist activity are roughly similar to those relating to non EU nationals.

10. The next proposal is to review the way in which people that have already been charged can be re-interviewed and recharged as further evidence is uncovered. In most terrorism investigations there is likely to be investigation and evidence gathering prior to arrest, followed by fourteen days for questioning. In this time it must be possible to bridge the small gap between the evidence needed to arrest and the evidence needed to charge. Once an initial charge has been brought the police and Crown Prosecution Service, they can apply to the Court to remand in custody as they feel appropriate.

11. It is necessary to look at the existing powers there are to re-question and recharge both to appreciate the scope of what is currently allowed, and to identify any amendments that might be appropriate. Under current legislation the police can arrest a terrorist suspect, question him for up to 14 days and then charge him. Normally once the suspect is charged, the police do not re-interview him. However, there is an exception provided under Paragraph 16.5 of Code C of the Police and Criminal Evidence Act 1984 which allows for re-interview (i) to prevent or minimise harm or loss to some other person, or the public (ii) to clear up an ambiguity in a previous answer or statement or (iii) in the interests of justice for the detainee to have put to them, and have an opportunity to comment on, information concerning the offence which has come to light since they were charged or informed they might be prosecuted. It is not clear that all cases involving terrorism suspects would fall into one of these categories. Therefore it might be appropriate to widen the list of exceptions. For example, an amendment to this provision could allow for re-interviewing in cases in which the Secretary of State considers it to be in the interests of national security or if the person is arrested in connection with terrorism.

12. It has never been the case that all the evidence to mount a trial must be in place before the suspect can be charged. All that is required is for the officer in charge of the investigation to reasonably believe there is sufficient evidence to provide a realistic prospect of conviction for the offence. If that is the case, then the officer in charge of the investigation informs the custody officer who is then responsible for considering whether the detainee should be charged.⁶⁰ Once the suspect has been charged there is nothing to stop the police from continuing their investigations in order to gather more evidence. The police will have ample opportunity to make enquiries into international terrorist networks, decrypt and analyse data held on computers, carry out forensic investigations and so on between charge and trial.

13. The point has been made by the Government that there is the potential for abuse as the police could bring an essentially frivolous charge, seek to remand in custody and therefore assure months of detention while seeking evidence for further charges. This might be true but misses the point that the potential for abuse is not in itself justification for not considering later questioning and re-charge where appropriate. We would hope that the police would not seek to abuse their powers and trust that magistrates considering bail will give proper consideration to the police case put before them. We raised the scope for re-interview and recharge not as a device which would allow easier detention of terrorism suspects but to demonstrate the range of options available.

14. Section 47 of PACE already allows for people to be bailed to reappear back at a police station while the police continue investigations. This is a commonly used technique to allow time for forensic examination (for example, the testing of a substance to see if it is a narcotic). We presume that section 47 powers would not usually be used in terrorism cases due to a concern that the suspect would abscond. This problem could be addressed by attaching conditions to section 47 bail. Conditions could include curfew, reporting, or the surrender of a passport. Defendants in criminal cases will frequently have restrictions placed on their bail. Similarly, section 1 of the Prevention of Terrorism Act 2005 (PTA) suggests a range of restrictions. Part of our objection and opposition to the provisions of Section 1 PTA was that they were applied as a punishment in themselves, were not made in anticipation of any criminal proceedings, and were potentially indefinite. If conditions were time limited and made part of criminal process by being imposed in conjunction with Section 47 PACE we do not imagine the same concerns arising.

15. We presume that one of the principle reasons why the police might have difficulty bridging the gap between the evidential standard required for arrest and that required for charge is the inadmissibility of intercept evidence in criminal proceedings. Liberty has never supported an absolute bar on the admissibility. The imperative for introduction seemed to be the protection of the Security Services' sources and methods rather than any obvious concerns for the fairness of the trial process. Legally the bar is an anomaly. The UK is the only country in the world, apart from Ireland, to have a ban. The Regulation of Investigatory Powers Act 2000 forbids the use of domestic intercepts in UK court proceedings. However, foreign intercepts can be used if obtained in accordance with foreign laws. Bugged (as opposed to intercepted) communications or the products of surveillance or eavesdropping can be admissible even if they were not authorised and interfere with privacy rights. There is no fundamental civil liberty or human rights objection to the use of intercept material, properly authorised by judicial warrant, in criminal proceedings.

16. If intercept evidence is admitted, existing rules of criminal evidence will apply to ensure that the case will not be unfairly prejudiced. Section 78 of PACE gives the court a discretion to exclude evidence if "having regard to all the circumstances, including the circumstances in which the evidence was obtained, the

⁶⁰ Police and Criminal Evidence Act 1984 Code C 16.1.

admission . . . would have such an adverse effect on the fairness of proceedings that the court ought not to admit it". At common law a judge has discretion "to exclude evidence if it is necessary in order to secure a fair trial for the accused."⁶¹

17. In addition, the doctrine of public interest immunity (PII) prevents material from being disclosed and adduced in the normal way, whenever it is held that the public interest in non-disclosure outweighs the public interest of full disclosure. Thus, if there are concerns over protection of the state's sources then the Crown Prosecution Service can make a PII application to the court to allow disclosure of certain evidence to be withheld from the defence and the public. This is particularly applicable when there are state interests that require protection or when informers and undercover sources have been used. There may be further practical issues to overcome, although these do not appear to have presented a problem in any of the countries where evidence is admissible. The Government has stated that it is not a magic bullet solution. This may or may not be true. Removal would, however, remove the primary obstacle to bringing trials in criminal cases.

Gareth Crossman
Director of Policy

Samantha Palmer
Research Assistant

19 December 2005

9. Memorandum submitted by Mark Morris

1. REQUEST

1.1 This submission follows a request received on 24 January 2006 in relation to two specific issues that form part of a larger case put by police before the inquiry.

1.2 In the limited time available, the issue of forensic analysis in relation to encrypted data will be addressed and also, as requested, some comments will be made in respect of the submission of Peter Sommer.

2. RELEVANT QUALIFICATIONS AND EXPERIENCE

2.1 I am Head of Forensics at LogicaCMG plc and manage their Computer Forensics Investigation Service ("CFIS").

2.2 LogicaCMG plc employs over 21,000 staff in 36 countries, and is listed on both the London (FTSE 250) and Amsterdam stock exchanges. The Company has a market capitalisation of three billion Euros, and is a major global force in IT systems and wireless telecoms.

2.3 As part of the Security Practice, CFIS provides computer forensic, expert witness, consultancy and investigative services to a wide range of clients such as Metropolitan Police Service, Department of Trade and Industry, as well industries in the nuclear, finance, transport and energy sectors. Forensic processes are conducted in accordance with the principles of the Association of Chief Police Officer's guidelines on the management of computer-based evidence—a document to which I have contributed. The Security Practice holds ISO 9001 quality assurance standard, has UKAS accreditation on its Evaluation Laboratories, CHECK accredited penetration testers and is BS7799 compliant in designated areas. All Security Services personnel are HM Government security cleared to at least "SC" level.

2.4 Formerly, I was a detective on the Computer Crime Unit at New Scotland Yard, before leaving in 1997 to work in the private sector. I was involved in some of the major computer crime cases of that decade, including the investigation of hacking into the global networks of a number of private sector international organisations as well as foreign government agencies. Such enquiries led me to work with a number of overseas law-enforcement agencies, and this complemented the training that I was, at this time, delivering for Interpol and at the Police Staff College.

2.5 Since my employment in the private sector, I have managed the forensic investigation teams on a number of high-profile cases; most recently the DTI prosecution in relation to the share tipping enquiry at the *Daily Mirror*.

2.6 By way of contrast, and balance, I am also instructed as an expert witness to the Military, Civil and Criminal Court by the Defence.

2.7 The views that I express are personal.

⁶¹ *Per* Lord Griffiths in *Scott v R*. [1989] AC 1242 at 1256. Since the enactment of PACE, this common law power is now rarely used.

3. SUBMISSION

3.1 Much has already been documented with regard to the forensic examination of computers, and it is not the purpose of this submission to regurgitate the large amount of material that is available in the public domain.

3.2 My submission is based on practical experience of managing complex enquiries and dealing with the forensic examination of computer media.

3.3 The existence of encryption on computer media can be categorised into the following general classes:

- Propriety encryption used by desktop applications such as email clients and office applications.
- Commercially available software encryption tools.
- Commercially available hardware encryption tools.
- Bespoke applications that can be engineered to suit a particular requirement.

3.4 In addition, technologies such as steganography and those involving drive volume manipulation (where the data is hidden as well as maybe being encrypted) can cause the forensic analyst sometimes insurmountable issues.

3.5 Whilst some encryption is easily broken, the increasing complexity of readily available applications can result in a lengthy period before the examination can have any success.

3.6 In the submission of Mr Peter Sommer, it is stated at paragraph 7 “Once the computer is in the hands of an examiner it is usually possible within a few hours to establish whether there is likely to be material of interest . . .” Whilst this may be the case in a simple investigation, this statement does not reflect the issues faced in a complex and serious enquiry. It may be the case, for example, that information gleaned in an interview, many days after the initial arrests, causes a re-examination of a piece of computer media.

3.7 Mr Sommer’s statement also pre-supposes that encrypted material is readily identifiable—it is not.

3.8 Although forensic tools have rapidly improved in terms of their power and speed, this has been matched by the huge increase in the capacity of computer media as well as the technical knowledge and ability readily available to serious criminals.

3.9 Mr Sommer continues (at paragraph 9) “A fuller examination might take . . . about 20 hours. The results at this time would certainly [be] more than enough for an initial interview and/or arguments for applications for continued detention.” Again, this may be true for one or two desktop computers, but this is not the case in a major enquiry. There is a risk here of a gross over-simplification of the issues that are faced by Police when investigating complex terrorist offences.

3.10 Where a number of arrests have been made, Police are likely to have seized a variety of different storage media which may require a number of different techniques to be used in breaking encryption and/or protection. This can range from simple personal identification numbers (PIN) on mobile phone cards to powerful commercial encryption on hard disk drives. In addition, biometric devices are increasingly common, and these bring further issues for the forensic analyst.

3.11 A competent enquiry requires the evidence to be looked at in its entirety, and the delay in attempting decryption of data does not simply affect that one piece of evidence; rather it has a negative effect on the whole picture that Police are trying to build.

3.12 In a recent (non-terrorist) case that we conducted, around 12 terabytes of data was seized and the forensic imaging alone took around 30 man-days in machine time. It is not that uncommon for Police (even in a residential environment) to discover a computer network that in its capacity would exceed that of a small business. Taken together with the increasingly common situation of data being stored at a third party location (via the Internet), I do not share the view that law-enforcement are able to gain an overview of the forensic evidence within a few days in the case of a complex enquiry.

3.13 Furthermore, the actual seizing of the relevant exhibits may take in excess of one day, especially where there may be a risk to life at the search scene.

3.14 At Paragraph 10, Mr Sommer states “. . . it should be remembered that computers are used to search the contents at great speed. . .”. In some of the work I have conducted, the best forensic tools available (running scripts provided by Police) simply could not cope “in one go” with the high volumes of data that we have had to process. The data had to be “batch processed” and this causes further delay. Accordingly, I disagree with the sentiments of his statement.

3.15 Furthermore the running of automated key-word searches does not remove the need for the time-consuming human element—where the results have to be analysed, placed into context and possibly translated.

3.16 Whilst modern forensic tools seem impressive in their speed and capability at examining data in the region of one or two hundred gigabytes, there are far more complex issues when searching data above this level. This is compounded when the forensic examiner has to deal with issues such as rebuilding forensic images of computer servers, and the sheer volume of data can mean that even getting the data into an examinable condition, can take several days.

3.17 Also, if there is a mixture of operating systems and storage technologies, then any examination is further delayed.

3.18 Such issues are further compounded when the investigation has to deal with an incomplete seizure of evidence. It may be the case, in a complex enquiry, that the successful decryption of data only points to the existence of other sources of evidence, which are yet to be located and seized.

3.19 In another case undertaken in December 2005, it was discovered that the suspects had been careful in saving all incriminating material to USB memory sticks, as opposed to the hard disk drive. These (easily disposable) memory devices had not been located by Police, and it was only through low-level cluster analysis of the hard disk drive media that it was possible to discover that they had even existed.

3.20 There are a number of ways to break encryption, and it is not the intent of this report to deal with the individual methods, whether technical or otherwise. The most common forensic tool used by Police is not very effective in even revealing encrypted data, and it is feared that many times such evidence may be overlooked.

3.21 The Internet has, of course, circumvented the ability of governments to reign in the availability of powerful encryption technology, and the “honeymoon period” for investigators is now over. It is now common to encounter some form of encryption on computer media seized as part of a criminal investigation, whereas five years ago, it was fairly unusual.

3.22 Suffice to say, the ability of the technically able and organised criminal to defeat a successful computer forensic examination through the use of encryption, has never been more available. In a complex investigation, even the most competent and well-resourced forensic laboratory can spend many weeks attempting to discover, decrypt and analyse the entirety of the computer-based evidence.

10. Memorandum submitted by the National Technical Assistance Centre

NTAC is a Home Office unit in the Crime Reduction and Community Safety group. Within NTAC the Forensic Computing Team (Stored Data) are responsible for providing technical support to UK law enforcement and intelligence agencies in order to assist them gain access to protected data.

NTAC forensics staff work on a diverse case load primarily associated with supporting the investigation of serious and organised crime. Typical tasks involve accessing encrypted files or password protected electronic devices.

Cases are submitted to NTAC via a Principle Points of Contact network comprising individuals usually working in the forensic computing or data recovery units of the respective customer agency.

Referred cases are generally a minimum of several weeks old by the time they are allocated to NTAC although casework involving crimes of a terrorist nature usually arrive more quickly. Delays occur for either or both of the following reasons:

- Limited resources within LE forensic teams This means that work is queued, sometimes for several months, awaiting an initial review by heavily tasked officers. It is only when this process takes place that encryption is recognised and NTAC contacted.
- Large amounts of data seized. In many serious investigations the sheer quantity of material needed to be examined means that it may take several weeks for the investigator to discover encrypted material.

On arrival at NTAC forensic case investigation starts immediately; even when total caseload is heavy, work is commenced on a new case within five working days.

An initial examination will reveal the extent of the encryption and indicate the likelihood of success. This process takes less than a week. The subsequent timing of the case is wholly dependant on the type of encryption applied and the nature of the forensic information recovered from the suspect computer. For example NTAC have processed cases for over one year and have still remained optimistic of obtaining a successful result. Other cases have been completed in less than a week.

In general terms however it would be fair to say that if resolution of a case had not been possible after a reasonable period then the likelihood of a positive result diminishes significantly. An exact value for the length of this period is hard, if not impossible, to determine precisely due to the variety of factors involved. Past experience has shown that two months is usually adequate if a result is possible although this might extend to three months where a substantial amount of data or a large quantity of computers and media are involved. After these timescales the case officer will, in most cases, have secured a result; have identified indicators which pointed towards a positive outcome with considerable further work or concluded that the chances of success were limited or non-existent.

11. Memorandum submitted by Mr Vinesh Parmar

This report is in response to the Committee's notice of 25 November 2005. Its purpose is to promote the understanding of Telecoms forensics and the investigative process thereon.

1. INTRODUCTION

This report has been produced from a forensic practitioner's perspective, to promote the understanding of the forensic data recovery of Mobile Telephones, the subsequent analysis and the investigative process. It has been compiled with prior consultation with practitioners in this field inclusive of Mr Greg Smith of Trew & Co and does not form any opinion for or against powers of detention. It is intended to remain unbiased throughout and is based on technical issues. A glossary of terms is attached as appendix 1 [*not printed*].

It is up to the committee to draw its own conclusion from this report with reference to terrorism detention powers.

2. QUALIFICATIONS AND EXPERIENCE

I specialise in the examination of computer and mobile telephone equipment for forensic purposes. I have been involved in this type of work since October 2000 and have conducted over 3,000 computer and mobile telephone forensic examinations to date. A full CV is attached as appendix 2 [*not printed*].

3. THE PRESENT TECHNOLOGY

The technology concerning mobile telephony has evolved over recent years at an alarming rate. A typical mobile phone or handheld wireless device is basically a mini computer. The communication aspects have greatly increased with the advent of "Smart Phones" and "3G Technology". We no longer have a simple communication medium, what we do have are handheld devices which can perform a multitude of tasks at a touch of a button.

A mobile telephone consists of the following components or data storage areas:

1. *SIM Card (Subscriber Identity Module—2g) or USIM (Universal Subscriber Identity Module—3g) Card*

The SIM/USIM is small printed electronic circuit board which allows connectivity to a valid service provider. The SIM/USIM predominantly holds the required network data to allow connectivity and communication; it also can contain user created data such as contact names and numbers, text messaging etc.

2. *Handset (internal memory)*

Advances in technology have allowed greater functionality of the handset itself. It is now common place for almost all devices to have an array of multi media capabilities as well as simple communication purposes. A typical handset can contain a vast amount of user data.

3. *Additional or Expandable Memory—Memory Cards*

In addition to the handset memory, the most common devices now incorporate expandable memory via the use of removable memory cards. Again a memory card can contain multitude of user data.

4. *Network services*

The network or service providers have also increased the functionality available to its subscribers thus increasing the type of information available.

4. DATA RECOVERY AND INVESTIGATIVE PROCESS

5. ISSUES WITH TELECOM FORENSICS

Present time Scales

On average a complete data recovery and presentation process for one device can take between four–eight hours, this is solely dependant on the device in questions and in some cases this time frame may be doubled or tripled. A number of well established forensic products exist to deal with the data recovery of SIM and USIM and the handset memory including memory cards. However with the rate of change with such technology these tools become outdated very quickly, thus the examiner is continually battling to identify the best suited method in line with best practice and rules of evidence to recover data, this again adds to the time scale. Where voicemail is encountered the process of retrieval is dependant on various factors, the retrieval requires the correct level of authorisation and limitations exist in terms of voicemail retention.

SIM/USIM Cards

The state of security or encryption on such devices is continually evolving. A SIM/USIM card can be PIN protected (Personal Identification Number), if the PIN is not known the only method to gain access is via the use of a PUK code (PIN Unblocking key) which is available from the relevant service provider. If this is encountered the time scales will be increased and will be based upon the time taken to obtain the relevant access code. This code will only be available with the correct legislative authority and providing the SIM/USIM in question is genuine and valid (not a clone or user created). Where a non UK subscriber is identified this process is further complicated thus the time frame is further increased and in some cases may not be available.

Mobile Handset and Memory Cards

The handset and memory cards are more complex to deal with. They can also be encrypted or protected via the use of a security code or password, this security feature in some devices can also be extended to the user's personal data such as messaging. If this code is not known it is not possible forensically to gain access to data. Brute force attacks are possible, however this process is labour intensive and may not yield any results. In some cases the device may be "locked out" if the incorrect code is applied. There are "flashing/hacking tools" available which claim to reset or bypass such security features, this process has its own complications. In terms of best practice and admissibility of evidence. The use of such tools is not recommended. If these tools were used it is possible that further legal issues materialise. It is possible that the manufacturers have a "back door" to reset or gain access to the device in question, it is unlikely that this information would be obtainable. The recovery of deleted data (Hex Dumps) from the device memory may be possible to a certain degree and is relatively a new practice, however this practice requires further extensive research to ensure the reliability and validity of such data for it to be evidential, this process has its own complications and limitations due to the various makes and models.

Investigative Process

6. THE FUTURE

The future of wireless handheld devices is growing rapidly. Convergence towards 4g technology is in the pipeline where we will see further capabilities. The list below identifies possible advances over the next 12-24 months.

- Increased security features.
- Increased memory—mini hard disks.
- More complex operating systems—Windows Mobile, Linux etc.
- Increased functionality (Digital TV/Satellite etc).
- Smaller devices (Wrist phones, wearable technology).
- Increased network services.
- Disposable devices.

The list above is not exhaustive but identifies the possibilities, which in turn will affect the way in which telecom forensics is undertaken.

7. CONCLUSION

This report has provided a brief insight into aspects surrounding telecom forensics and the future of wireless mobile devices. It is evident that we will see a rapid increase in the use of mobile devices as a form of every day communications. It is also known that such devices are used frequently to facilitate criminal activities. As the scope of this technology increases so do the complications concerning telecom investigations principally the resources needed and time scales required in conducting such investigations.

23 January 2006

12. Memorandum submitted by Evan Price

1. I strongly believe that Parliament is sovereign and that Members of Parliament are not delegates but representatives of the people. The constitutional conventions of Parliament have evolved to try to ensure that the servants of the executive are impartial and have no part to play in the adversarial nature of the political discourse. Time and again, this Government has blatantly ignored those constitutional conventions, especially where its arguments have been found wanting by the press.

2. The latest example of this Government's determination to ignore constitutional convention is in the apparent encouragement by the Home Office that senior police officers contact their local Members of Parliament to persuade them to vote in a particular fashion on a controversial issue relating to the proposed power that the Police be able, subject to unspecified controls by the judiciary, to hold individuals for up to 90 days in cases where those individuals are suspected of participating in specified offences relating to terrorism.

3. In this submission, I will not deal with the rights or wrongs on the proposed power. Although I have served in Northern Ireland as a part of the security forces (a very minor role at a very junior level), I do not profess to have any relevant or current expertise in relation to the fight against terrorism that would assist the Committee. My concern relates to the lobbying of Parliament by elements within the Police and the encouragement of that lobbying by Ministers. If my views are correct, then both Ministers and senior police officers have acted wrongly and, I suggest, unconstitutionally.

4. There is a constitutional convention that when serving soldiers, naval or air force personnel wish to involve themselves in politics, they are required to cease to continue in the employ of the Crown. This constitutional convention extends to requiring officers of the services to resign their commissions. Over the years, many service personnel have disagreed with Government policy and have had to fight their conscience and decide whether to continue in the service of the Crown or resign. What none have been permitted to do is to continue in the service of the Crown and campaign against a particular Government policy. This convention has resulted in the clear feeling that service personnel are independent and will serve Governments of different political persuasions "without fear or favour". It has meant that we have never had a General or Admiral standing for election whilst serving the Crown.

5. When at law school, I understood that a convention in substantially the same terms extended to the Police service. There are some differences that relate to the fact that the Police are, so often, involved in activities that have a great impact on the community they serve. Inevitably, they evolve and develop a keen interest in issues relating to law and order and want to express a view as to how their powers and duties can best be enhanced. They have developed structures and bodies (such as ACPO and the Police Federation) that have large publicity departments, and on many occasions their interventions (whether individually or collectively) have been both useful and beneficial.

6. The difficulty in relation to the Police conduct in relation to the 90-day detention issue arose in the context of individual Ministers and senior police officers asserting that the Police view of the need for the power was more important than the views of individual Members of Parliament who were not persuaded by the arguments. In my view, the step at which a police officer, whilst retaining his or her position, tells an MP to vote in a particular fashion on a particular issue, is the step at which the police officer ceases to be impartial. He or she compromises the impartiality of his or her office and demeans the service that he or she is a part of.

7. The Government's response to criticism of this nature was for the Home Office Minister Hazel Blears to say that it was "entirely appropriate" for police to make the case for detaining terror suspects for up to 90 days (as reported by the BBC and others). For the Minister not to see the danger in the police acting in the manner troubles me. The fact that Ministers appear to have encouraged this breach of impartiality is especially concerning. Ministers are Members of Parliament first and Ministers second. The fact that they had lost the argument with the opposition parties and a significant number of the Labour party was not a reason for them to encourage, or possibly cajole, police officers to breach the impartiality of their office and demean their police service. In addition, by breaching the constitutional convention, and by encouraging that breach, the individual police officers and Ministers have acted unconstitutionally.

8. The benefits of the constitutional convention are to be seen where the police are trusted as impartial servants of the executive (please note that I do not use the word "servant" in any prejudicial sense whatsoever). If the impartiality is compromised, then elements of the community who believe that they are the target of police action or police surveillance gain an excuse for not accepting that the police are impartial. This risk in the context of the 90-day detention power is that, if, after further consideration, Parliament concludes that the powers are required, elements within the Muslim community in Britain may decide that the Police cannot be trusted; this is a price that must not be paid, and in my view is not worth paying.

9. The contrast between the conduct of individual police officers and ministers can be contrasted with that of the director of public prosecutions. On the radio (I believe that it was the Today programme on Radio 4 about 10 days ago), I heard the Director asked for his views. The gist of his response was to say that his advice was in the public domain and that he would not tell Parliament how to weigh that advice against all of the other evidence and advice that was before Parliament. He said that he was sure that the Members of Parliament would make their choices after considering all of the evidence and that the vote was a matter for Parliament. If only all of the servants of the executive were as aware of their constitutional obligations to act impartially and to be seen so to act.

13. Memorandum submitted by the Secretary of State for the Home Department

The Government is grateful to the Home Affairs Committee for carrying out this important inquiry and for the opportunity to submit written evidence.

SPECIFIC CASE FOR 90 DAYS PRE-CHARGE DETENTION IN TERRORIST CASES

The case for extending the maximum pre-charge detention period in terrorist cases to 90 days has been set out by Ministers during the course of the debates on the Terrorism Bill and by the police, most notably in Andy Hayman's letter of 6 October 2005.

The Government has nothing further to add to what has been said previously. In the course of the Third Reading debate in the House of Commons on the Terrorism Bill, I indicated that the Government accepted the decision taken on this matter by the House of Commons.

JUDICIAL OVERSIGHT OF EXTENDED DETENTION

Pre-Charge detention for terrorist suspects is currently supervised by specially designated District Judges (Magistrates' Courts) at Bow Street Magistrates' Court. While the Government is confident that they have been performing this duty highly professionally, it sees the case for increased supervision of the period of detention pre-charge. The Bill provides for detention beyond the current 14 days to be sanctioned by a High Court judge who will have all the facts of the case before him. The police will need to provide full justification of continued detention. The Government believes that the involvement of the higher judiciary will bring fresh and rigorous supervision to any extended period of detention.

RESOURCES FOR POLICE AND INTELLIGENCE SERVICES

The Government is absolutely committed to ensuring that the Police Service is effectively funded to meet its Counter Terrorist commitments. In 2005–06 specific CT funding for the Police Service in England and Wales amounted to £96 million of revenue and £8 million capital of which £61 million revenue was allocated to the Metropolitan and £35 million Revenue and £8 million capital was allocated to provincial forces. This compares to the 2002–03 figures of £59 million (£47 million MPS and £12 million provincial forces).

In the 2004 spending review the Security Service received an average increase of around 60% over baselines. This will allow for a growth in capacity and for staff numbers to increase from around 1,800 in 2001 to 3,000 in 2008.

I think it is also important to recognise that resources of themselves are not a complete solution. During his appearance before the Joint Committee on Human Rights on 24 October, Peter Clarke, Deputy Assistant Commissioner, Head of the Metropolitan Police Anti-Terrorist Branch and National Co-ordinator of Terrorist Investigations was asked specifically about this point:

“**Q72** Dan Norris: Is it fair to say that some increase in resources would help and therefore perhaps the three-month detention period is still too long?”

Mr Clarke: No, it would not. However many resources we had I do not think it would cut into the basic problem here, which is the sheer weight of material which we are routinely recovering in these cases. This has to be analysed at some point and then focused into an interview strategy and an investigation strategy set by the senior investigating officer. At some point one person has to be aware of what is emerging from all this data. It cannot just be a cavalry charge.”

LESSER CHARGES

The Government believes that there are a number of problems with the suggestion that charging with a lesser offence would be a suitable alternative to extending the period of detention.

The most fundamental of these is that it will not always be possible to bring a lesser charge. There may simply be no usable evidence which sustains a charge until, for example, an encrypted computer has been cracked.

If the charge is a minor one there is a possibility that the person will be granted bail and will be freed either to abscond or commit a terrorist crime. As some have suggested, it may be possible to change the rules surrounding bail but changing the presumptions surrounding bail or allowing matters unconnected with the offence for which a person has been charged to be taken into account at a bail hearing would be both difficult and probably very contentious.

Bringing lesser charges may also hamper the process of the investigation. The first few days of any investigation are crucial. It would be very unfortunate if the police were required to divert attention from

investigating a terrorist crime just so they could gather sufficient evidence to bring a charge of, say, benefit fraud against a suspect.

I also wonder whether this approach would offer less protection for the suspect. Under the Terrorism Act continued pre-charge detention is subject to regular judicial oversight and can only be granted if the Judge is satisfied that it is necessary and that the investigation is being conducted as expeditiously as possible. Once a person had been charged with a lesser offence there would not be the same imperative on the police to move so quickly.

Finally, there must be doubts about the honesty of this. Bringing lesser charges as a ruse simply to keep someone in custody smacks of abuse and I dare say many people would condemn other countries which operated in this way.

USE OF TAGGING, SURVEILLANCE OR CONTROL ORDER AS ALTERNATIVES TO CUSTODY

Again I do not believe that these options would be suitable way of treating those arrested for serious terrorist crimes. The person may know that it is only a matter of time before evidence implicating him in terrorism comes to light so if he is released into the community he may feel he has nothing to lose by carrying out a terrorist act.

Tagging does not physically prevent a person from carrying out an act. It may be possible to establish that a person had breached his curfew but that could be after the person has committed a terrorist act. If a person seeks to remove his tag a signal will be sent to a control centre but by the time the police have arrived on the scene he may have disappeared.

Unless a person's dwelling is surrounded by a team of police officers around the clock, control orders and surveillance can not guarantee 24 hour protection. There will always be a possibility that a person who is subject to a control order evades the control and is then able either to disappear or to carry out a terrorist act.

QUESTIONING POST CHARGE

As has been made clear during the Parliamentary passage of the Terrorism Bill, the Government is willing to look again at the issue of post-charge interviewing to see if the current provisions in paragraph 16.5 of PACE Code C (Detention, treatment and questioning of persons by police officers) best suit the needs of achieving a successful outcome to an investigation. We intend to publish a consultation paper on this issue in Spring 2006. That paper will also consider the existing caution provided for in Code C, paragraph 16.5 and the potential for amending that to the caution given to a suspect during the pre-charge of the investigation.

However, post charge interviews are only relevant if it has been possible to lay a charge in the first place. They cannot therefore be a substitute for extending the maximum pre-charge detention period.

INTERCEPT AS EVIDENCE

My Written Ministerial Statement on 26 January 2005 on the outcome of the review of the use of intercept as evidence made clear that the use of intercept as evidence is not a "silver bullet". The review showed that there may be a modest increase in convictions of some serious criminals but not terrorists. For example it would not have made a difference in supporting criminal prosecution of those were detained under the powers in Part 4 of the Anti-terrorism, Crime and Security Act 2002. It is also important to recognise that not all cases involve intercept material. Even if such a change could be made it would not apply in every case and could not therefore, of itself, remove the need for an extended pre-charge detention period. For these reasons, intercept as evidence would not remove the need for an extended pre-charge detention period.

In the light of the review of the use of intercept as evidence, we concluded that the risks of changing the law to allow it outweighed the benefits of doing so. The review noted in particular that new technologies would revolutionise communications in the UK over the next few years and that now was not the right time to move to an evidential regime. A current study into the impact of these technologies on interception will report to Ministers shortly.

The Government will continue to keep the ISC informed of significant developments in this area.

Rt Hon Charles Clarke MP

12 December 2005

14. Supplementary memorandum submitted by the Secretary of State for the Home Department

I am grateful to you for giving me the opportunity to appear before your Committee on 21 March to give evidence to your inquiry into terrorism detention powers.

In responding to a question from Richard Spring, I said I would write about his understanding that we would be happy to use intercept provided by foreign intelligence agencies as evidence. The statutory prohibition on the use of intercept as evidence only applies to UK warranted interception, not to intercept product obtained by other jurisdictions. The reasons which I have given about the difficulties in using domestic intercept product as evidence clearly do not apply to foreign product.

You may be interested to know that we are aware of only very rare instances of other jurisdictions using the product of their intelligence agency (as opposed to law enforcement) interception as evidence in courts. Any such product provided by those jurisdictions to the UK is likely to come with strict conditions and restrictions about its use and handling by our own agencies.

In answer to a question from David Winnick I said that I could not recall whether any Muslim organisation has specifically lobbied me in favour of the proposal to extend the maximum pre-charge detention period in terrorism cases to 90 days. I have subsequently checked and can confirm that there has been no such lobbying.

In part this may be because there have been a lot of inaccurate scare stories about the Terrorism Bill and its effects. I can confirm the accuracy of the figures which I had supplied in my earlier written evidence of the number of people who have been held for between seven and 14 days.

Rt Hon Charles Clarke MP

27 March 2006

15. Memorandum submitted by Gregory Smith

This is a submission in response to the Committee's Notice of the 25 November 2005 with respect to the most recent request for further comment Notice 11 January 2006 relating to mobile telephones evidence. This submission is intended to provide general and technical observations.

A1. PRIMER

It is intended that this submission will inform the Committee about mobile telephones evidence in order to aid interpolation of witnesses from the various agencies, ministries and any other witnesses that may be called to this Enquiry. This is with particular regard to timescales, resources and the practicalities involved with disclosure.

For the avoidance of doubt, this submission neither argues for or against the detention period currently being considered by the Committee.

A2. QUALIFICATIONS & EXPERIENCE

Principal of Trew & Co, consulting forensic engineer (18 years) and Chief Training Officer Trew MTE.

1. MOBILE WIRELESS TECHNOLOGY

When generally referring to mobile telephone it is in fact reference to a mobile station (MS) that actually comprises two devices, a mobile telephone and a smart card.

Mobile Telephones (Wireless devices)

A mobile telephone first and foremost is a digital wireless data device in its own right. It has been suggested a mobile telephone is first and foremost a computer, which is misleading, not only from the point it usurps the laws of physics, but legally as well. Mobile telephones are recognised in European Directives (Telecommunications Terminal Equipment Directive 91/263/EEC, particularly the provisions of Article 4, and the Radio and Telecommunications Terminal Equipment (RTTE) Directive 99/5/EC). The provisions of European Directives applied for recognition of the technology, harmonisation and removal of trade barriers and other requirements. National laws (Communications Act 2003, Telecommunications Act 1984 (parts of which have been repealed) and the Wireless Telegraphy Act 1949 provisions are applied to this technology. There are applicable Statutory Instruments as well. National law are applied to protect sovereignty over the spectrum, permission and purpose of use (the opposite being hijack of the airwaves), protection against interference, law interception and so on.

Behind, but supporting the aerial and radio circuitry, a mobile telephone has computer architecture in order to action commands and receive response from the radio network and devices connected to it. It also has a memory for the retention of user content. The purchaser owns the handset and there are various makes and models of handset available. There are broadly speaking two categories of mobile telephones separated into two categories:

The first is a GSM mobile telephone containing a number of user features and functions. The second is a Smart Phone mainly used on GPRS and 3G networks, which is rich in features and functionality. The two categories of devices fall under the above legislation. A third possibility may arise which is a computer data device (PDA or laptop), which is not a handset wireless device, but makes use of the radio network by using a wireless card inserted into it. The wireless card as a device falls under the above legislation. Where the PDA has permanently fixed wireless (GSM/3G) capability the above legislation applies to it.

Mobile Telephones and Smart Phones are required to have a tamper-proof serial numbers called an IMEI (International Mobile Equipment Identity) numbers, which are electronically embedded into the mobile telephones security. *** It is common to find on mobile telephones and smart phones passwords that users can invoke to prevent unauthorised persons gaining access to particular folders or files. Access codes that simply activate particular programs subscribed to by the handset user may be used in smart phones. Overcoming this form of security entry level may not be possible without co-operation from the user and/or the third party application vendor.***

The data storage found in a GSM mobile telephone or mid-range smart phone is approximately between 2Mb to 4Mb of data, which can print out to many hundreds of A4 sheets of paper.

Smart Card (SIM and USIM)

SIM (Subscriber Identity Module) card is a user-friendly title to give provenance to the smart card used for the GSM communications, but SIM does not actually define the device. Technically speaking, a SIM card comprises two parts:

A physical card, it comes in two sizes, a credit card size and a plug-in card—the size of postage stamp. Both have electronic circuitry, micro-controller and computer operating system and termed an Integrated Circuit Card (ICC), which is assigned a unique Identity (ID), hence ICCID. This identity is a serial number that one might find helpful to think of as a car chassis number. That being the case, it may be equally helpful to think of the user's mobile telephone number as a car vehicle registration plate number.

The ICCID number is electronically embedded in the card and is recorded externally on the face of a SIM card where it is referred to as the SIM Serial Number (SSN).

There are important responsibilities attached to the ICCID number. Most importantly, when a SIM Card is supplied to a subscriber in order that the subscriber can make or receive mobile telephone calls using the subscription details recorded in the SIM, the card becomes a Charge Card. A benefit acquired and a detriment incurred by user and network operator by its use. For that purpose the implementation and structure of the ICCID number is recorded in the International Telecommunications Union Telecommunications Recommendation—ITU-TE118 International telecommunication charge card numbering scheme.

Turning now to SIM which it is entirely different from the ICC. Whereas ICC is considered the physical device, the SIM is a Module, which is programmed onto the card, where user content, services and network data can be recorded and stored. SIM's memory structure is similar to the memory tree one see in Windows Explorer. SIM has a Main Directory, Sub Directories, Folders and Files.

An example of network data found in SIM, it contains the subscriber's identity called the IMSI (International Mobile Subscriber Identity) which is linked to the user's mobile telephone number. Without the IMSI recorded in the SIM the IMSI would not be transmitted for registration to and validation by the mobile network, thus the user would not be able to make or receive calls. The IMSI is important in criminal investigation as it enables law enforcement to gain access to subscriber details, billing and call records and so on. Another example, but this time about user data found in SIM, are SMS text messages, which may have been either sent or received by the user. These can form an important aspect in a criminal investigation and highlight contacts and communications between parties that may be linked to a crime.

The data stored in a GSM SIM card be approximately 0.25Mb, which roughly translates to about 100–150 A4 sheets of paper.

USIM (Universal Subscriber Identity Module) card is the title used to give provenance to the smart card used for 3G communications and, like SIM, the USIM title does not actually define the device. USIM card comprises:

Universal Integrated Circuit Card (UICC) card is the physical device containing electronic circuitry, micro-controller and computer operating system, and the card follows the principles of International charge card numbering scheme (ITU TE 118). It comes in two sizes, a credit card size and a plug-in card—the size of postage stamp.

Unlike SIM ICC used for GSM, UICC was designed for use in generic markets such as transport, finance and loyalty, physical access, healthcare, mobile communications and so on. The UICC may be used for one market or for use with several markets. For instance, mobile communications and Banking are two markets that have already attracted market implementation.

Also UICC was designed to cater for access to more than one digital wireless technology, thus contains the necessary modules for 3G WCDMA mobile network and the 2nd generation mobile technology, GSM module.

The Data storage in the UICC card is much larger than a SIM card, about 0.5Mb. If one were to print out the quantity of data applicable to UICC, USIM and GSM this can typically run to on average nearly 200-300 A4 sheets of paper. In any criminal investigation, attendance time to deal with this amount of data runs into days.

The USIM/s module/s, and there can be numerous modules for USIM based upon the number of accounts to which the user subscribers, coupled with a GSM module, means this smart card uses multi-platform data sharing. What this means is that data found in the GSM module might mean the data can be used by the USIM/s module/s as well. Consequently, investigation of the data residing on the card adds further support for the examination of data running to days, not hours.

If the above wasn't enough to deal with, UICC has two primary security codes with up to 16 supplementary codes that may be shared between two or more applications or data files. Further complications arise, for example, with Banking where having used the access code to initiate the Banking application, a further access code (session password) is needed to access the account information which is remotely stored at the Banking website. This access code needs to be transmitted to the mobile network and on to its destination address along with the subscriber profile to be validated and authenticated before access to the remote account will be allowed.

Wireless Networks

There are currently four generations of digital wireless development used by devices in operation in the UK. GSM (Global Systems for Mobile) communications, a pan-European TDMA (Time Division Multiple Access) digital technology that has been adopted and is used globally. GPRS (General Packet Radio Switching) which is an overlay wireless technology using the GSM network as its backbone, but provides high speed data transport for data-rich content (Internet etc) and adopted by some countries globally. 3G, known as WCDMA (Wideband Code Division Multiple Access) was developed as an International standard. The UK has a separate radio network for GSM and 3G (WCDMA), although this is not discernible by the ordinary user and functions just the same, save that 3G provides for multimedia services and functions from voice calls, text and email to Internet, video, TV and radio. Lastly, WLAN (Wireless Local Area Networks) to enable access to emails, Internet etc in hot spot areas, such as cafes etc.

Summary

The above overview provided, albeit, a brief introduction to mobile telephones and smart cards. What we know is mobile communications has evolved between 1992–2006 but that evolution continued at an alarming rate. This means that examining data in handsets and smart cards is taking longer and overcoming the security access to get to the data inside is getting harder, not easier.

Moreover, distribution of data is not always via the mobile network but by use of very short range wireless protocols such as Bluetooth, which operate at up to 10 metres between devices. This means data can be generated in mobile telephones and smart cards and consumes a large amount of attendance time to discover where the data originated. Further complications are mobile communication devices enabled with 4G technology—referred to as WLAN. Smart cards, too, are developing fast with new ways of communicating, such as RFID (Radio Frequency Identification) for close range toll ticketing (useful for payment scheme suitable for transportation such as Oyster on the London Underground). This adds a further dimension to, and layer of, evidence requiring attention.

I have outlined below some issues associated with examining devices, security access, data used for criminal investigation, time factors for retrieval, possible conflicts with legislation, and defence issues that I thought the Committee may wish to know. Should the Committee wish to know more or wish me to expand upon the issues in this document then please let me know.

It has not been possible to cover every issue regarding mobile telephone examination and evidence in this document. For instance, this document has not discussed timescales or delays associated with handling and pre-examination techniques (fingerprinting, DNA, etc) that may need to be dealt with before setting about the task of extracting and harvesting data from the devices.

2. MOBILE TELEPHONE EXAMINATION

Mobile telephone and SIM card examination is not simply about extracting and harvesting data from these devices. The primary concerns about evidence is to ensure integrity of the evidence from start to finish. Evidence said to be obtained for intelligence purposes no longer follows the principle it will not be used in criminal proceedings. Any evidence obtained must be safely acquired and stored on the basis that it might be used as evidence, even if it is not used straightaway. In consequence, seizing a mobile telephone and examining it straightaway has a high risk of contamination. Consequently, a number of procedures are required to avoid as best possible contamination of evidence:

- Seizure procedure.
- Handling and device assessment procedure.
- Goods inwards procedure (presented for examination).
- Laboratory Environment procedure.
- Examination procedure.
- Post-examination procedure.
- Quarantine procedure.

There are many subset-procedures to each of the main procedure categories, above.

The procedures evolved as the number and variety of mobile telephones and SIM cards increased and due to a disparate range of devices connecting to or with mobile telephones and SIM cards, such as flash memory cards, PDAs, laptops etc. Each of the devices has their own memory where user content can be retrieved. ***

Following examination the harvested data is then examined and analysed to link the data to a particular crime or to discard it. It takes as long to analyse data and to discard it as it does to analyse the data to comprehend its relationship to a crime.

3. EXAMINATION—SECURITY ACCESS

PIN 1 (Personal Identification Number)

SIM and USIM have the capability to be locked where the user invokes a four-digit code to prevent access to the SIM card content and services. If the user does not volunteer or provides an incorrect PIN 1 preventing access to the device then SIM/USIM needs to be unlocked—PUK 1.

PUK 1 (Personal identification number Unlocking Key)

PIN 2 (Personal Identification Number)

The user as a further step in security personalisation invokes PIN 2 to be activated as a four-digit code. It is used to bar certain numbers being dialed or only allowing certain numbers to be dialed. If the user does not volunteer or provides an incorrect PIN 2 preventing access to the device then SIM/USIM needs to be unlocked—PUK 2.

PUK 2 (Personal identification number Unlocking Key)

Universal PIN, Global PIN and Local PIN

These are security access conditions introduced for 3G UICC/USIM. It is not absolutely clear yet whether all smart card manufacturers will introduce all the PINs for their UICC cards. However, as these matters are laid down in the 3G standards unlock procedures are in place ***

Third Party Vendor PINs

3G USIM PIN codes for Banking applications, payment schemes, access to particular Internet sites etc do require the user to transmit a PIN code and user ID and the user ID and code to be validated and authenticated before gaining access. ***

Handset Passwords

An alpha-numeric password activated by the handset user and can be applied to entry level to the handset functions and content or can be applied to prevent access to particular content (phonebook, SMS text messages etc). ***

Handset Application Passwords

This type of user password can be invoked to activate a particular application, where application offers security access conditions. ***

4. EXAMINATION—DATA ACQUIRED FOR CRIMINAL CASES

Below is a general list of data that can be extracted and harvested from smart cards and handsets in criminal investigation:

Smart card

- ICCID number/SIM Serial Number
- PIN/PUK
- IMSI (subscriber identity)
- Mobile Telephone Number
- Subscriber's Home Network
- SIM or USIM Service Table (allocated and activated services)
- Roaming Networks
- Forbidden Networks
- Access to various networks technology
- Location data
- Broadcast Control Channel data
- Service Dialed Numbers
- Barred Dialed Numbers
- Fixed Dialed Numbers
- Last Numbers Dialed
- Outgoing Call Indicator (outgoing calls)
- Incoming Call Indicating (answered/unanswered calls)
- SMS text messages
- Deleted text messages
- SMS Service Centre number/s
- Voicemail platform number/s
- Voicemail indicators
- Phonebook numbers
- Global Phonebook (3G)
- Mailbox indicators

Handset

- IMEI number
- Battery Power
- Clock settings
- Application settings
- Applications
- Passwords/Keylocks/SIMLock
- Phonebook
- Last Numbers Dialed
- Last Numbers Received
- Last Number Missed

- SMS text messages/MMS messages
- Deleted text messages
- Emails
- Video/Images
- Voice tags
- Voice recording/Dictation/Music
- Internet/WAP/GPRS setting
- Organiser/Calendar
- Extended Memory cards

5. EXAMINATION TIMESCALES

SIM/USIM

The average time to extract and harvest data from GSM SIM using forensic tools is approximately 5–10 minutes. To analyse the data can take several hours.

The average time to extract and harvest data from 3G USIM using forensic tools is approximately 20–30 minutes. To analyse the data can take five hours to 24 hours or even longer dependent on the data to be assessed.

Handsets

The average time to extract and harvest data from a standard GSM mobile telephone using forensic tools is approximately two hours for specific data and four hours for full recovery dependent on quantity of data on handset. To analyse the data can take 15 hours dependent on the data to be assessed.

The average time to extract and harvest data from a GSM smart mobile telephone using forensic tools is approximately four hours for specific data and eight hours for full recovery dependent on quantity of data on handset. To analyse the data can take 24 hours dependent on the data to be assessed.

The average time to extract and harvest data from a 3G smart mobile telephone using forensic tools is approximately six hours for specific data and 15 hours for full recovery dependent on quantity of data on handset. To analyse the data can take 48 hours dependent on the data to be assessed.

Handset Application Passwords (Third Party Vendors)

Standard forensic examination tools do not recognise these types of programs/applications and therefore require manual examination of handsets. ***

Extended memory cards

The average time to extract and harvest data from a flash card extended memory using forensic tools is approximately two hours for specific data and eight hours for full recovery dependent on quantity of data on 1Mb cards. To analyse the data can take 10 hours dependent on the data to be assessed.

The average timescales given above are based solely upon examiner set up, device set up, device communication protocols and data output format.

6. EXAMINATION DELAYS (ADDED TO EXAMINATION TIMESCALES)

SIM/USIM PIN locked: UK issued card can take 24 hours to 90 days to obtain PUK code from mobile network operator.

Handset Passwords: ***

Handset (no SIM/USIM card): where handsets are seized with no SIM/USIM card, manufacturer's privacy procedure can be invoked that can either prevent access to handset using normal methods or deletes data in call registers and bars access to phonebook etc. Engineering SIM/USIM required from handset manufacturer. This can take up to 30/60 days to obtain dependent on co-operation from handset manufacturer, particularly foreign manufacturers without an UK base.

Handset Application Passwords (Third Party Vendors)

Password locked applications can be entirely independent of the handset manufacturer and therefore this can present difficulties in obtaining access codes or they may not be obtained at all.

Application Session Passwords

Accessing third party vendor applications represent one difficulty and another is a session password required for use with the application in order to gain access to data held remotely at a website. This can cause further delays in obtain the session passwords.

Encoding Schemes

Encrypted Voice Data

Conversation recordings or dictation facilities on handsets are encrypted by the handset's security for each make and model. It is common to find simply extracting the data file containing this content is difficult to unravel the encryption on a computer, as the computer does not have the same security software and files that reside in the handset. The examination process can be extended by a day, having to use the seized handset and replay and digitally record conversation or dictation stored in the handset.

7. OTHER DELAYS (BEYOND EXAMINATION TIMESCALES)

It is said there is no substantive evidence of a mobile communication having taken place without corroboration to the mobile network operators billing records, call records and any stored communication data. Obtaining this information from the mobile network operator can take a day to weeks. There can be numerous reasons for this.

Pay As You Go

These are not subscriber accounts where a bill is sent to the user. The data resides in mobile call records, which needs to be obtained via account details. Where the account has not been used for quite some time, it may be the call records have been deleted after a year.

Communication Data

Content sent or received, such as voicemail, text, images etc may only be saved by the operator for a short period of time. This can add delays where a mobile telephone and/or SIM/USIM card has multiple communications data stored in it or them.

Inter-Network Records

As is known 3G operators can run their call traffic over several competitive networks. Hutchinson 3 has used O2 to assist with voice and data calls. ***

8. ADDITIONAL ISSUES

Defence

As an observation only, it is a common statement made by solicitors and barristers that they do not understand the complexity of mobile telephone evidence. It is as likely that detained person/s may not understand it either. It appears odd then that there has been no mention of mobile telephones linked to a detained person/s where the telephonic evidence has been independently assessed or challenged. Does this mean where the blind are leading the blinding, either the evidence is being accepted at first instance without independent assessment, or is the evidence being ignored on behalf of the detained person/s?

As law enforcement has raised the issue of mobile telephone evidence contributing to delays, the Committee may consider it a good idea that a Register be compiled with names of independent mobile telephone experts, like myself (engaged by prosecution and defence over 13 years). The Register can be used by defence solicitors specialising in this area so that they can pro-actively engage experts to give a fair assessment of the technical evidence that is to be used or is being used against the detained person. Firstly, an independent expert could assess the matter and accuracy at first instance. And, or, secondly where reasons being given for delays to a person/s detention, said to be caused by mobile telephone evidence,

perhaps the independent expert may indicate whether a more expedient method or path exists to obtain evidence. The Committee may consider that a Court might consider the opinion of the expert as a way of determining between genuine delays and unnecessary delays.

29 January 2006

16. Supplementary memorandum submitted by Gregory Smith

As you may recall during the Select Committee inquiry it was mentioned about the lack of skills and experience for examining and handling mobile telephone evidence. Below are the list of Trew MTE courses, which will now include for 2006 knowledge skills and experience that will take account of Committee's public inquiry.

I thought the Committee may wish to see mine and others comments at the inquiry were not just statements, they can be put into practice.

LAW ENFORCEMENT

Trew MTE runs numerous courses that are device specific and general.

NOTE 1:

Whilst GSM (Global System for Mobile) communications is a Pan-European standard (at since inception 1991) it has gained global appeal and adopted in many countries around the World. Given its global adoption GSM is now a global digital wireless standard. GSM is known as 2G (Second Generation digital wireless technology system).

NOTE 2:

3G (Third Generation digital wireless technology system) is a development of the 3GPP (Third Generation Project Partnership) that brings together international operators and device manufacturers. Whilst 3G has been technically realised and technically implemented (rolled out for use) it is still evolving as a multi-media digital wireless system and its global adoption is expected (when compared with GSM) to take about 10 years. 3G it is said is an International standard.

1. GSM SIM (Subscriber Identity Module) Card Courses

- 1.1 Introduction to SIM card examination course (2 day course).
- 1.2 SIMIS version 1 (2 day course).
- 1.3 SIMIS version 2 enhanced (2 day course).
- 1.4 PhoneBase version 1 (2 day course).

2. 3G USIM (Universal Subscriber Identity Module Card Courses

- 2.1 Introduction to USIM card examination course (2 day course).
- 2.2 USIM Detective version 1 (2 day course).

3. Mobile Telephone (handset device) courses

- 3.1 Introduction to Mobile Telephone Examination course (2 day course).
- 3.2 PhoneBase 2 (2 day course).

4. GSM Cell Site Analysis

- 4.1 GSM Mobile Telephone Network Overview (1 day course).
- 4.2 GSM Cell Site Identification (2 day course).
- 4.3 Site Survey (2 day course).
- 4.4 GSM Cell Site Testing (2 day course).
- 4.5 GSM radio test measurements (2 day course).

5. *Interpreting Mobile Communications Data Course*

5.1 Interpretating evidential data from GSM handsets and SIM card (2 day course).

5.2 Interpreting evidential data from GSM network call records (2 day course).

Gregory Smith
Chief Training Officer
Consulting Forensic Engineers
Trew MTE

23 March 2006

17. Memorandum submitted by Peter Sommer

1. This is a submission in response to the Committee's Notice of 25 November 2005. It seeks to assist by providing some technical background to two issues:

- the examination of computer disks and encrypted material thereon; and
- how telephone interception takes place and related issues of disclosure and admissibility.

2. It is hoped that this will enable the Committee to have more informed exchanges with witnesses from the relevant agencies and ministries, particularly in relation to timescales, resources and practicalities of disclosure.

QUALIFICATIONS

3. A full CV appears as Appendix I [*not printed*]. I am a Research Fellow at the London School of Economics specialising in information security and digital evidence. I have acted as an expert witness in many cases involving digital evidence since 1985—these have included Official Secrets, Terrorism, narcotics trafficking, paedophilia, fraud, large-scale software piracy, murder and global computer misuse. I am Joint Lead Assessor for Computer Examination in the scheme run by the Council for the Registration of Forensic Practitioners.⁶² I am an external examiner for the Master's course at the Centre of Forensic Computing at RMCS Shrivenham and have provided training to the Crown Prosecution Service and to police intelligence analysts as well as advice to the main high tech law enforcement training centre in Bedfordshire. I am the author of *Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence* published by the Information Assurance Advisory Council.⁶³ I was a Specialist Advisor to the Trade and Industry Select Committee before and during its scrutiny of the Electronic Communications Bill (HC 862/Session 1998–99)⁶⁴ which was the original locus of legislation on encryption—later transferred to the Regulation of Investigatory Powers Act, 2000. During my work for the Select Committee I visited the then interception facilities at the National Criminal Intelligence Service (NCIS).

4. For the avoidance of doubt, this is a personal submission.

EXAMINATION OF COMPUTER HARD DISKS

5. Reliable techniques and procedures for the forensic examination of the hard-disks from computers have been established for over 15 years. The first *Good Practice Guide* published by the Association of Chief Police Officers (ACPO) appeared in 1998; the current version is the Third Edition.⁶⁵ It enunciates principles and provides detail to address evidence preservation, continuity and auditability. Hard-disks are carefully copied in their entirety ("imaged") so as to include apparently empty sectors which might contain deleted material and examination, both by investigators and defence experts, then takes place on copies of the original.

6. There are well-established products to handle both the initial imaging and the subsequent analysis.⁶⁶ Types of analysis include: examination of substantive files, extraction and display of all potential picture files, email, Internet activity, the use of computers to search for words and distinctive patterns (such as for credit cards), etc across, the entirety of a disk, the development of chronologies of activity. There are extensive opportunities to recover deleted material—and these too are subjected to the same forms of analysis.

⁶² <http://www.crfp.org.uk/>

⁶³ <http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v08.pdf>

⁶⁴ <http://www.parliament.the-stationery-office.co.uk/pa/cm199899/cmselect/cmtrdind/862/86202.htm>;
<http://www.parliament.the-stationery-office.co.uk/pa/cm199899/cmselect/cmtrdind/648/64802.htm>;
<http://www.parliament.the-stationery-office.co.uk/pa/cm199899/cmselect/cmtrdind/187/18707.htm>

⁶⁵ Available for download from: http://www.nhtcu.org/media/documents/publications/ACPO_Guide_for_computer-based_electronic_evidence.pdf

⁶⁶ For example, EnCase, AccessData FTK, Sleuthkit

7. Once a computer is in the hands of an examiner it is usually possible within a few hours to establish whether there is likely to be material of interest—based on indications of the computer’s sophistication in terms of configuration and usage, other information obtained at the time of seizure and other intelligence.

8. A fuller examination might take, though we are in “length of a ball of string” territory here, about 20 hours. The results at this time would certainly more than enough for an initial interview and/or arguments for applications for continued detention.

9. Production of exhibits in evidential form and formal witness statements might take longer.

10. Although hard-disk sizes are increasing all the time, it should be remembered that computers are used to search the contents at great speed; it is possible to index the entire contents of several hard-disks in a case and thereafter get almost instant results from specific searches.

POLICE RESOURCES

11. However all these timings depend on the availability of appropriate skilled and equipped technicians. Based on membership of the First Forensic Forum and the Digital Detective Bulletin Board, I estimate there to be approximately 5–700 competent examiners in the UK though the numbers in current direct police employment are probably only 200–250. Numbers vary considerably between similar police forces—Kent employ 16 specialists, Essex two. The largest single category of investigation relates to images of child abuse. Large-scale recent cases have created long delays before hard-disks can be examined. There are currently limited ring-fenced funds for computer forensics, not universally applied, but this scheme is likely to end sometime in 2006. When SOCA comes into formal existence, NHTCU which provides the lead for training standards will be part of it, but will no longer be part of the police, though the regional forces and the Met (with its specialist ant-terrorist unit) will be “police”.

12. The Committee should ask tough questions about the resources available and associated time delays.

DEFENCE ACCESS

13. Copies of hard disks from which material is extracted are themselves evidence and are made available to defence experts. “Unused” material is available under regular disclosure arrangements. The detail can be seen in the current *CPS Disclosure Manual*.⁶⁷ Where hard-disks contain sensitive material a defence expert may be asked to provide undertakings in addition to those implicit in the role; undertakings may be re-inforced with a related court order. In rare circumstances a defence expert may have to work at designated law enforcement premises; there may then be significant additional cost implications for the Legal Aid fund. My own experience is that while negotiations for access are sometimes difficult, they usually end in a mutually satisfactory conclusion.

ENCRYPTED MATERIAL

14. The existence of encrypted material on a hard-disk is normally self-evident, if not immediately readable. Normally software providing the means to encrypt and decrypt will also be found.⁶⁸ It is possible to hide data on a hard-disk and/or within files on a hard-disk—the general name for this steganography. Techniques exist to detect steganography even if immediate decoding is not possible. Such detection is normally not a very lengthy process, once the initial suspicion has been formed.

15. Plainly the existence of encryption and steganography on a hard-disk without reason and/or production of decoding facilities are grounds for suspicion and application for extended detention.

16. Techniques for decryption, depending on circumstances, fall into four broad categories:

- some encryption facilities are relatively easily broken either for lack of complexity or poor implementation. Decryption facilities for these are available commercially and it is reasonable to suppose that the National Technical Assistance Centre (NTAC), the main regular law enforcement body for this activity, has all of these and more. Times to decrypt may vary from near-instantaneous to a few hours;
- where stronger encryption facilities are in use, a forensic examination of the hard-disk of computers used to originate or receive the material may provide clues in the form of “in clear” versions of encrypted material and passwords/keys;
- whilst most people using encryption prefer to rely on established products, it is possible that every now and then new packages may be encountered. It is not possible to put a figure on the time required to “break”, though as above, forensic examination of associated hard-disks may provide clues. But few “new” encryption systems turn out to be robust;

⁶⁷ <http://www.cps.gov.uk/legal/section20/chapter-a.html>

⁶⁸ The software provides the means to encrypt and decrypt—the individual encryption key for each session is also required.

- failing this, brute force or modified brute force methods such as dictionary attacks (successive trying of potential passwords) may have to be deployed using extensive computing resources. This may take significant amounts of time and may fail.
17. I hope the Committee will seek from relevant witnesses information about:
- quantities of encrypted material encountered in relation to overall computer evidence obtained; and
 - figures for the various qualities of encryption and time to decrypt using the classification above.

INTERCEPTION COMMISSIONER REPORT

18. I draw attention to the most recent Report from the Interception Commissioner (2004).⁶⁹ At para 7 he says:

However, the use of information security and encryption products by terrorist and criminal suspects is not, as I understand, as widespread as had been expected when RIPA was approved by Parliament in the year 2000. Equally the Government's investment in the National Technical Assistance Centre—a Home Office managed facility to undertake complex data processing—is enabling law enforcement agencies to understand, as far as necessary, protected electronic data.

19. A curiously identical statement appears in the 2004 Report of the Intelligence Services Commissioner.⁷⁰

THE LAW AND ENCRYPTED MATERIAL

20. Part III of the Regulation of Investigatory Powers Act 2000 (RIPA) provides powers for investigators to issue notices requiring disclosure of “protected”, that is, encrypted data⁷¹ and for punishment for failure to do so.⁷² The specified penalty on conviction is two years.

21. The Committee would do well to probe why this existing legislation has never been enacted. My own understanding is that Home Office officials drafted detailed proposals which covered not only stored data (as on a hard-disk or CD) but also data in transmission. While this second is desirable in terms of completeness of coverage it appears the proposals conflicted with actual practices employed *inter alia* by the secure networks used for high value financial transactions. Discussions became bogged down in detail and little attempt was made to produce legislation and regulations limited to stored data, which would have had few problems of implementation and addressed the largest and most obvious category of encrypted material of interest to investigators.

INTERCEPTION

22. Interception of the content of telephone calls, emails, etc is admissible in common law but excluded by statute—currently section 17 RIPA 2000. Consensual interception is admissible and so is interception material lawfully acquired outside UK jurisdiction. The aim of the current policy is said to safeguard methods and facilities and was explained in a Home Office consultation paper of June 1999.⁷³ The general effect is to allow interception warrants but to deny their existence for court proceedings—this applies to both prosecution and defence. The detail of how this is handled appears in the CPS *Disclosure Manual*⁷⁴ and I hope that the Committee will press the CPS and others hard to assess its effects—the *Manual* acknowledges many difficult areas of judgement.⁷⁵ The Committee should also review carefully the relevant Attorney General's Guidelines in relation to section 18 of RIPA.⁷⁶

23. Communications/traffic data—who called whom, when and for how long—is admissible under Part I Chapter II RIPA 2000. Such evidence is often produced in conspiracy trials to demonstrate a common purpose among a number of people. Commercially available software packages to identify patterns aid this exercise and produce persuasive graphics.⁷⁷ Data traffic also includes details of which cellphones were registered to which specific base stations thus bringing the geographic locations of individuals into evidence—this is called cellsite analysis.

24. There are frequent occasions when the production of evidence based on data traffic together with other evidence before the court makes it wholly obvious that interception has taken place, though neither prosecution nor defence are allowed to refer to it.

⁶⁹ <http://www.official-documents.co.uk/document/hc0506/hc05/0549/0549.pdf>

⁷⁰ <http://www.official-documents.co.uk/document/hc0506/hc05/0548/0548.pdf>

⁷¹ S 49 ff, RIPA 2000.

⁷² S 53 RIPA 2000.

⁷³ Apparently no longer on the Home Office website.

⁷⁴ <http://www.cps.gov.uk/legal/section20/chapter-a.html#148>

⁷⁵ <http://www.cps.gov.uk/legal/section20/chapter-e.html>

⁷⁶ <http://www.cps.gov.uk/legal/section20/chapter-a-annex-i.html>

⁷⁷ For example, *Analyst's Notebook* by I2.

THE TECHNOLOGY OF TELEPHONE INTERCEPTION

25. There is nothing complicated or secret in the principles of how interception of landline and cellular phones take place. Two elements are required: the voice component (by placing simple circuitry across the line or by capturing digitally) and the “traffic” component—who called whom, when and for how long—which is part of the regular record of the telecommunications company for revenue collection and quality of service purposes and already admissible.

26. Good practice, along the lines used for preserving hard-disk evidence, suggests that the voice and the traffic components (referred to in the literature as the IRI, Intercept-Related Information) should be forensically inextricably linked as a test against tampering and editing. The details, as adopted by very large numbers of jurisdictions and also used in international law enforcement, are explained in a technical document published by the European Telecommunications Standards Institute (ETSI) Security Techniques Advisory Group dated 2001.⁷⁸ There is no reason why a *Good Practice* Guide, similar to that for computer evidence⁷⁹ should not be devised and published; indeed it would probably be less complex and concentrate on continuity and auditability.

27. It might be helpful to take in turn each of the claimed arguments against making interception evidence admissible:

- *sensitive methods would be disclosed* The existence of regular interception facilities can hardly be secret—they are referred to in the legislation and the annual reports of the Surveillance Commissioner⁸⁰ and the ETSI documents are public. Defence lawyers are not able to embark on fishing expeditions but must comply with the rules emerging from the Criminal Procedures and Investigations Act, 1996 (as amended, particularly by the Criminal Justice Act 2003⁸¹). Specific disclosure would only follow a detailed and consistent defence case statement. The prosecution have the ability to question the quality and *bona fides* of a defence expert and there are opportunities to seek undertakings and court orders in respect of defence experts. This is already done in terms of hard-disk evidence. It is unlikely that defence experts would need to enquire about overall capacity to intercept (which probably should be kept secret) as their questions will be focused on the reliability and integrity of specific tendered evidence and related “unused” material. Whilst overwhelmingly most interception will use regular methods there may be a few instances in which unorthodox techniques are deployed and which it is desired to keep secret—but the authorities can still make use of the Public Interest Immunity (PII) certificate mechanisms—judicial and ministerial—to exclude these.⁸² Applications for PII certificates can also be made where it is desired to disguise the role of co-operation from other national intelligence and law enforcement agencies;
- *there would be significant additional overheads* RIPA already requires that detailed records are kept of interception warrants and their usage.⁸³ Without such records the Interception Commissioner cannot do his work.⁸⁴ Data storage problems would be significantly less than those resulting from the seizure of hard-disks;
- *the privacy of innocent 3rd party individuals would be placed at risk* It is certainly true that, if interception becomes admissible in order to demonstrate the integrity of an interception some innocent conversations involving third parties will need to be retained for the duration of criminal proceedings either as evidence or as “unused” for the purposes of disclosure obligations. The current practice⁸⁵ is to destroy any such material as soon as possible. But the position is no different for emails found on computer hard-disks. Since such emails have been received by the computer owner they are not “intercepted” for the purposes of Part I Chapter 1 RIPA and so are admissible. Prosecution and Defence experts will see these as part of the process of checking the integrity of the disk evidence preservation process. But, unless they are relevant, no one else will and both experts will be under duties of confidentiality imposed by their job functions and by duty to the courts.

⁷⁸ <http://webapp.etsi.org/exchangefolder/es—201671v020101p.pdf>

⁷⁹ http://www.nhtcu.org/media/documents/publications/ACPO_Guide_for_computer_based_electronic_evidence.pdf

⁸⁰ Who refers to the sites he visits and provides statistical information: <http://www.official-documents.co.uk/document/hc0506/hc05/0549/0549.pdf>

⁸¹ Part 5.

⁸² http://www.cps.gov.uk/legal/section20/chapter_a.html#049,
http://www.cps.gov.uk/legal/section20/chapter_a.html#210

⁸³ RIPA 200 Part I Chapter 1.

⁸⁴ <http://www.official-documents.co.uk/document/hc0506/hc05/0549/0549.pdf>

⁸⁵ Home Office Draft Code of Practice.

THE TECHNOLOGY OF DATA INTERCEPTION

28. So far we have simply been concerned with interception of telephones—landline and cellular. Because the “voice” and “traffic data” elements are so obviously separate it is easy to understand how to handle the distinction made in RIPA⁸⁶ between content and communications data. But interception in the data world of the Internet means, in the instance, capturing all the data packets associated with an Internet identity and then attempting to filter them according to whether they appear to be “traffic data” (for example the “header” in terms of email) or “content” (the message itself). There is little clarity, for example, with how one would make the distinction in web-based email such as Hotmail and the facilities offered by large Internet Service Providers (ISPs) such as BT Internet. The problem becomes even greater as conventional telephony is replaced by Voice over Internet Protocol (VoIP) telephony and the use of Instant Messaging grows.

29. It is obviously beyond the scope of your current enquiry to investigate such matters: there are significant cost and regulatory implications to ISPs but my immediate point is that increasingly there will be disputes about interpretation of RIPA—and these disputes will inevitably require disclosure of material which may later be declared inadmissible for being “content”, an impossible situation.

LEGISLATIVE IMPLICATIONS OF ADMITTING INTERCEPTION

30. My arguments refer to interception for any type of crime, not just terrorism. Any review of the law would need to consider, among other things, whether authority for warranting should be transferred away from the Secretary of State to the judiciary and also the extent to which interception material alone, without additional corroboration, should ever be sufficient to permit a conviction.

7 December 2005

18. Supplementary memorandum submitted by Peter Sommer

This is an addendum to my earlier submission dated 7 December 2005 in response to the Committee’s Notice of 25 November 2005. The Committee decided to extend the period for submissions so that they could gather wider views on such technical aspects as time required to examine computers, issues of encryption, mobile telephony and arguments about returning intercept material into regular admissibility.

The addendum is prompted by some of the remarks made in the submission of AC Andy Hayman of the Metropolitan Police Anti-Terrorist Branch.

I hope the Committee will feel able to accept this addendum and find it useful.

1. Time taken to examine computer material In his “theoretical case study” AC Hayman says: “The High Tech Crime Unit say that every computer hard drive seized during that period of time takes a minimum of 12 hours to image for the assessment teams at Paddington to then provide to the interviewing officers”. In fact there is no need, in the first instance, to image a hard-disk in order safely to carry out a preliminary assessment of its contents—which is what is needed for interview. The most popular computer forensics product used in the UK, EnCase has a “preview” facility which prevents a hard-disk of interest being written to while it is being examined; the examiner can still recover deleted files and carry out sophisticated searches. Alternative means of previewing disks include the use of specially set-up Compact Disks⁸⁷ and specialist hardware which absorbs any attempt at writing to a suspect disk⁸⁸. In all these circumstances the disk is available for examination within a few minutes. Imaging only becomes necessary when the hard-disk is to become evidence but is not necessarily needed in the early days of an investigation.

2. In any event 12 hours for a single disk is something of an exaggeration. Modern imaging products claim rates of up to 5GB/per minute— so that even a comparatively large hard-disk of 120 GB would be imaged in 30 minutes. The only real problems are with some laptops where direct access to a hard-disk may be difficult. AC Hayman may like to consult more closely with his technicians.

3. Elsewhere AC Hayman says: “The examination and decryption of such vast amounts of data takes time, and needs to be analysed before being incorporated into an interview strategy. This is not primarily a resourcing issue, but one of necessarily sequential activity of data capture, analysis and disclosure prior to interview.” Whilst recognising much of what he says it would be productive for the Committee to enquire whether the police are using the quickest methods of dealing with large quantities of potential disk-based evidence—and weighing the costs that these might imply against the costs, tangible and reputational, of holding suspects for long periods without trial. In particular, my own experience is that in situations where large numbers of computers are seized, only a small proportion of them turn out to be relevant in terms of an enquiry. Thus, it should be possible to use numbers of relatively lower-skilled investigators and technicians to eliminate the irrelevant and filter upwards those of potential interest.

⁸⁶ Specifically ss 20 and 21(4)(a).

⁸⁷ eg Helix, FarmerDude.

⁸⁸ eg Voom Technologies ShadowDrive.

4. Audio Probe Evidence. I also wish to add a little to my observations about the admissibility of intercept evidence. Use is made in terrorism, narcotics and trafficking of audio probes, in other words, bugs. This evidence is admissible, though a warrant for intrusive surveillance is required.⁸⁹ Many of the arguments adduced to prolong the inadmissibility of communications intercept evidence apply with more force to bugs—publicity about technical capabilities and danger to individual technicians⁹⁰ in terms of having to go into hostile locations in order to set up the equipment. As I have sought to show, where domestic terrorism is concerned, there is little secret about how intercepts are carried out (at points provide by telephone companies) or how (by technicians throwing a switch or two). But bugs need to be planted and the precise capabilities of bugs in terms of sensitivity, distance between bug and listening point and life (dependent on batteries or other form of power) are not well known. The police are usually able to persuade judges to grant Public Interest Immunity certificates and this may be a pointer to how they would deal with defence disclosure requests in respect of techniques of interception.

27 January 2006

19. Memorandum submitted by Chris Sundt

1. This is a submission in response a supplementary request via the Parliamentary Office of Science and Technology (POST) to the Committee's Notice of 25 November 2005. It seeks to assist by providing further technical background on the following issue:

- the need to decrypt computer files; and
- the length of time needed to obtain and analyse data from mobile phones.

2. It is hoped that this will enable the Committee to have more informed exchanges with witnesses from the relevant agencies and ministries, particularly in relation to timescales, resources and practicalities in these areas.

3. Qualifications. A full CV appears as Appendix 1 [not printed]. I have 40 years experience in the IT industry. I have been involved in information security since the early 1980s. I retired from ICL in 1999 as a Senior Consultant with emphasis on information security.

I now work part-time as an independent consultant on information security with specific interest in security policy/architecture, e-crime legislation, secure electronic commerce, and cryptography policy. In this role I have worked for major commercial organizations and government departments (including Intelligence Services) on a variety of tasks. I currently act as rapporteur for the EURIM Working Group on e-crime issues. I represented Industry on the Project Board that established the National Hi-Tech Crime Unit (NHTCU) and on the NHTCU Strategic Stakeholders Group. I contribute actively to the debate on legislation relating to e-commerce and e-crime and on the need for a cross-Departmental National E-crime Strategy. I was actively involved in the discussions at the OECD and elsewhere on national and international policies on controls on cryptography, and also contributed to what is now Part III of the RIP Act on access to cryptography keys and to the debate on data retention. I have given papers on a variety of security related topics at conferences and seminars in the UK, Europe and the USA and contributed to OECD, G8, European Union and national working groups.

4. For the avoidance of doubt, this is a personal submission. It reflects personal experience and knowledge drawn from my current and past activities.

5. The Need to Decrypt Computer Files The need to decrypt computer files will depend in large part on the context within which that data was obtained as part of an investigation. It will usually be found associated with other data:

- On permanent storage associated with seized computers. This permanent storage could be internal or external fixed discs, USB memory sticks, CD-ROMs, CD-DVDs or the like. It can be assumed that the associated computer system includes the software used to access that storage, and that there are associated papers and other material seized at the same time.
- On portable media found on premises searched, or on individuals arrested.
- Obtained by other means—usually legal interception.

6. It must be assumed that when data is seized a systematic investigation of both the tangible⁹¹ and computer-based material is carried out in parallel to look for evidence supporting the case against the suspect(s).

7. As has been documented elsewhere (for example the submission to this Committee of Peter Sommer) there are well-established techniques for examining different sorts of computer-based material.⁹² Part of this process will distinguish three types of data:

⁸⁹ Under s 32 RIPA 2000.

⁹⁰ See the remarks of Baroness Park, *Hansard* 7 March 2005, and indeed on other occasions: <http://www.publications.parliament.uk/pa/ld200405/ldhansrd/pdvn/lds05/text/50307-41.htm>.

⁹¹ Here taken to mean paper records, photographs, music CDs, etc.

⁹² The Directors and Corporate Advisors Guide to Digital Investigations and Evidence, published by the IAAC, provides a good guide to computer forensic processes and what information can be obtained from computer systems.

- That irrelevant to the investigation (for example, standard software).
- Easily readable information potentially relevant to the investigation that warrants further examination.
- Data that appears unintelligible without further specialist work.

8. Potentially relevant information can be found in a wide variety of places in computer storage outside the content of files directly accessible to a user.⁹³ Examples include meta-data, directory data, configuration data, audit and logging data, backup files, and forensically recovered information (including deleted files, swap files and the like).

9. The effort required to examine in more detail potentially relevant information can, in itself, take significant time and resource (both skilled personnel and equipment). Whether additional effort needs to be expended on interpreting unintelligible data will depend on two key factors:

- The extent to which examination of the tangible evidence and of readable material from computer systems affects the case against the suspects.
- The proportion of data seized that is initially unintelligible.

10. The Committee should understand how often examination of readable material alone affects the case against suspect(s), and on what basis the decision to spend significant resource on interpreting unintelligible data is made.

It should also understand the extent to which lack of appropriate skilled resource and equipment inhibits the timely examination of computer-based material.

11. Data can appear to be unintelligible for a variety of reasons, such as:

- It has been written in a file format with which the computer forensics staff and/or their tools are not familiar. Where the associated computer system has been seized, the relevant software should be found on that computer, but needs to be run in a controlled environment to ensure data is not lost or corrupted. Where the format is not known, it may require research to ascertain what software was used to create the data and how.
- The data has been compressed or otherwise encoded to save space. It is usually trivial to decompress such data unless the compression technique used is not well-known, in which case additional work needs to be done to determine the nature of the compression algorithm. It is reasonable to assume that the National Technical Assistance Centre (NTAC), the main body supporting law enforcement for handling unintelligible data, has extensive experience of handling compressed data.
- The data has been encrypted in some way.

12. The Committee should ask what proportion of unintelligible data is susceptible to straightforward techniques such as de-compression and what proportion is actually encrypted.

13. The remainder of this submission considers the methods to, and time to, decrypt information where the examination of other material, both tangible and computer-based, has not provided sufficient evidence to affect the case against the suspect(s).

14. It is commonly supposed that the only way to interpret encrypted data is to analyse it directly, but this need not be the case.

15. In most cases the software (or hardware) used to encrypt the information will be known as it will be associated with the computer system(s) with which the encrypted data was found. Such products can have implementation weaknesses that can be exploited and/or the supplier can provide information to assist this process. It is reasonable to assume that NTAC is well aware of all such techniques and more. Times to decrypt can vary from near-instantaneous to a few hours or days.

16. Just because data is held in encrypted form does not mean that a copy in unencrypted form does not exist elsewhere in a computer system. As mentioned earlier, there are data files created in a computer system other than those visible to a user. Many products hold working copies of data, the system may hold data in caches or temporary files, and so on. Detailed examination of such data may uncover unencrypted copies of data, as may forensic analysis of discs—for example, recovering deleted working files containing unencrypted versions of data.

17. Often people write down their keys and careful examination of tangible material may find copies of keys on paper, in diaries, etc. In some cases the key may be held on a separate token, such as a smart card.

18. Keys have to be held somewhere securely in a way that enables them to be used. It is often easier to attack the underlying key management system, gaining access to the user keys⁹⁴ than to attack the encrypted data. Once these keys are known, it becomes routine to decrypt the associated files. Forensic examination of the associated computer system may enable user keys to be recovered given knowledge of the way the keys

⁹³ Typically, the words and figures in a document or report, images, designs within an application file, a database or selection, emails, webpages, files downloaded.

⁹⁴ There are products that enable the escrow of keys, providing an authorised exceptional means of access. Such escrow mechanisms can be set by default.

are secured by the product used.⁹⁵ Where this uses a password/pass-phrase there are well-known techniques available to attack them that can take from a few minutes to days (depending on the complexity of the password or phrase). There are known techniques for obtaining user keys from commonly available products and from tokens (such as smart cards) with which it is reasonable to assume NTAC is familiar. Times to obtain keys in this way can vary from near-instantaneous to a few hours or days depending on the complexity of the key management system.

19. The efficiency of so-called brute-force attacks⁹⁶ depends on the crypto algorithm used and the length of the associated keys. Mathematically-based crypto algorithms used by computer systems are continually subject to analysis with people looking for weaknesses that can be exploited by cryptanalysts to reduce the possible number of keys that need to be tried. It is reasonable to assume that NTAC is familiar with known weaknesses in commonly used algorithms (and in the way that specific products implement them) that can be exploited to reduce the time for a brute-force attack.⁹⁷ If the algorithm used is not well known this can take significant time or may fail.

20. While it is probable that most people will use commonly available products it is possible that from time to time unfamiliar products will be encountered. If the supplier can be identified it may be possible to establish sufficient knowledge on how it works, and its weaknesses, to enable a successful cryptanalysis attack. Detailed forensic examination of the associated computer system may also provide clues as to how it works. This will all take time, and it may not be possible to provide a decryption capability within any reasonable timeframe.

21. The Committee should understand how often each of these approaches is used to provide the plaintext of encrypted data. In particular, the Committee should question how often plaintext or keys are found using commonly available techniques.

22. Where encrypted data is found on portable media not associated with a particular computer system it is often possible to determine the product used to encrypt the data by forensic examination of the media. If this is not the case it may be difficult to decrypt the data in any reasonable time.

23. The Committee should understand what proportion of encrypted data is found on portable media not associated with any seized computer system.

24. While the above discussion applies predominantly to data encrypted with a key, the underlying arguments apply equally to other forms of hiding data, including steganography. It is reasonable to assume that NTAC is well aware of the common ways for handling data hidden using such techniques, including exploitation of weaknesses in underlying products and methods.

25. The Committee should understand the proportion of “encrypted” data found that uses techniques other than classic encryption, such as steganography, and the extent to which NTAC is resourced to address such techniques.

26. The above discussion addresses primarily stored data. Encrypted intercepted data (including data held in temporary storage during communication—for example at an intermediate ISP) presents additional issues. Such data may be encrypted in different ways:

- The data may have been encrypted as a file and communicated in its encrypted form.
- The data may be encrypted by the originating application (such as email) to be decrypted by the receiving application.
- The data may only be encrypted between the ends of a communications link, but remain in clear in the networks and computer systems at either end (link encryption). If the data being communicated is already encrypted, such a link will encrypt that data again.

27. Whether such data can be decrypted will depend on where it was encrypted originally. Many systems encrypting at the link level use protocols that generate random session keys that are discarded after use as the data is in original form at either end. As no keys are retained, the only direct means of decryption is by brute force. One or more computer systems at either end of the link may provide access to the plaintext that was communicated and/or, for application-encrypted data, to the encrypted data and to relevant keys, access to which would be as described earlier.

28. The Committee should seek information in two areas:

- What proportion of intercepted data is encrypted.
- Of that data, what proportion is also available in the originating and/or receiving computer systems, making direct decryption of the intercepted data irrelevant.

⁹⁵ As one example, I have personal experience of commercial products that have held crypto keys in clear in system files, making decryption of any data encrypted using that product trivial.

⁹⁶ In essence a brute-force attack tries all possible keys in an attempt to obtain the plaintext from encrypted data. It usually requires knowledge of the decryption algorithm and of the length of the key.

⁹⁷ Success against Enigma was in no small part due to the ability to reduce the number of possible keys that needed to be tried for the messages for a specific day to manageable proportions because of weaknesses in the way the device was employed.

29. Overall, the need to decrypt computer data depends substantially on the extent to which examination of readable data affects the case against the suspect(s) and the basis on which it is considered the encrypted data will, when decrypted, contain relevant information.

30. Although I am not a lawyer, I do not see the link between the need to decrypt data and the ability to charge a suspect within the detention period. As far as I am aware a person can be held on lesser charges while the investigation proceeds, and more serious charges made later if appropriate. This process would seem to be dependent on the overall significance of the material seized, and not just on timely decryption of encrypted material.

31. Resources The discussion above assumes adequate resource with the appropriate skills and technical equipment to carry out the level of computer forensic analysis required to enable rapid progress on investigations with significant amounts of computer-based data. Law enforcement is currently woefully under funded to support the required levels of resource with the capability of individual local police forces varying widely from the very competent to the barely capable.

32. The launch of the National Hi-Tech Crime Unit (NHTCU) in 2002 was a first step towards developing a national capability for investigation of computer-related crime (albeit with funding significantly less than that requested as the minimum necessary). Over the past 4 years it has provided funding directly to local police forces to ensure that each has at least a basic capability in computer crime investigation. It also provided a centre of excellence to support such work particularly for level 3 crime. However, the minimum level of investment in the NHTCU, and the lack of incentives for local Chief Constables to invest in computer crime units has resulted in a significant backlog of work in investigation of crimes involving computers. Just one major investigation (such as the recent paedophile case—Operation Ore) can absorb almost all available skilled computer forensic resource.

33. The funding in 2006–07 for the NHTCU and for computer crime units through the NHTCU has been reduced significantly leading to concern that even the current level of capability cannot be sustained. NHTCU will be part of SOCA from 1 April 2006, but it is not clear what future investment SOCA will be making in this area, or how it will support local police forces. It is not clear what incentives local police forces will have to invest in their computer crime units once NHTCU funding ceases.

34. The lack of investment in skilled resource (people and equipment) nationally and within local police forces is a major constraint on the timely examination of computer-based material. The need for such investment is not helped by the lack of any knowledge of the amount of computer-based material potentially associated with crimes of all sorts, not just terrorist activity. There is no such information collated upon which to base a case for greater investment in computer forensics and investigative skills.

35. The Committee should seek information on:

- The historical investment in, and plans for future investment in, the capability both nationally (including SOCA) and in local police forces for computer forensics and investigative skills and equipment.
- The methods of collecting data that can be used to justify future investment in such resources both nationally and locally
- The backlog of work awaiting computer forensic analysis and investigation, and the ability to handle a major investigation without severely impacting ongoing investigations.
- The investment in NTAC justified against the amount of encrypted material expected to need analysis over the next few years.

26 January 2006

20. Memorandum submitted by UKERNA

1. This is UKERNA's written submission to the Home Affairs Committee's Inquiry into Terrorism Detention Powers. UKERNA is the not-for-profit company that manages the operation and development of the JANET computer network connecting universities, colleges, research establishments and schools to each other and to the global Internet. This submission considers only issues relating to the recovery of information from encrypted computer files and the time required to achieve this.

SUMMARY

2. Four different approaches to obtaining information from encrypted computer files are considered:
- legal compulsion of the system owner or other person;
 - finding traces of decryption activities through normal forensic investigation;
 - brute-force decryption of the material; and
 - brute-force or intelligence-led attacks on decryption key passphrases.

If the material was both encrypted and accessed by people highly skilled in the use of encryption then none of these approaches appears likely to reveal information without many years of delay; however if the encryption systems were chosen or ever used without scrupulous care then it appears likely that information would be revealed on a similar timescale to a normal digital forensic investigation.

DETAIL

3. There are at least four different approaches that might be taken to recover information from encrypted files on a computer. These are considered in turn.

4. The simplest approach is to require the owner of the computer, or some other person with access to the decryption keys, to decrypt the material or provide the key necessary to do so. Powers to require this, backed by the criminal sanction of up to two years imprisonment if a person refuses to comply, are contained in Part III of the Regulation of Investigatory Powers Act 2000, sections 49 to 56. However, despite the apparent benefits for investigating authorities, these provisions have never been brought into force.

5. If the encrypted file has ever been decrypted on the computer then there is a reasonable likelihood that information left over from this activity may be found by normal forensic investigation. This may include clear text versions of part or all of the file, unprotected versions of decryption keys or passphrases to unlock those keys and thereby make them available. Many of the routine processes running on a computer will cause accidental copies of this and other material to be retained, for example as deleted files, in filespace related to printing or where the content of memory has been temporarily saved to disk. Well written encryption tools will try to reduce the likelihood of this happening, or to remove such traces when they do occur, however these also require scrupulous care by the operator to ensure that they do not accidentally create additional saved information.

6. Probably the hardest method is to attempt a direct decryption of the material by guessing the cryptographic key. Using encryption products generally available at present it is likely to take decades or centuries to blindly guess and test a significant fraction of the possible keys, and no algorithmic methods have been published that would significantly reduce this time.

7. A more productive approach is likely to be to attempt to defeat the protection applied to the decryption key. In most encryption systems the key used for decryption is much too long for a person to remember. This key is therefore usually stored as a computer file, itself protected by a further layer of encryption whose key can be remembered. This protection key is often expressed as a password or passphrase which may be guessed; the difficulty of doing this will depend on the training, skill and care of the person who created it and the person who must remember and use it. Guesses may be based either on computer algorithms generating large numbers of possible passphrases, or on information known about the person or found on the computer. In theory a good passphrase will be as hard to guess as the key it protects and therefore either approach will still take many years to have a likelihood of success. In practice the passwords and passphrases chosen by people are much easier to guess than this and it is common for more than half of the login passwords chosen by users of any computer system to be guessed by a computer program running for an hour or so. Clearly a skilled user should be able to choose a much better passphrase than this, and these could take years to defeat.

19 January 2006

21. Memorandum submitted by Professor Brian Collins

1. This is a submission in response to the Committee's Notice of 25 November 2005. It seeks to assist by providing some technical background to two issues:

- the need to decrypt computer files; and
- the length of time needed to obtain and analyse data from mobile phones.

I am Professor and Head of Department of Information Systems at Cranfield University based at the Defence College of Management and Technology (previously known as RMCS) at Shrivenham.

2. For the avoidance of doubt, this is a personal submission. I have added commentary on the submission of Dr Peter Sommer within my text and referenced his submission accordingly.

3. The first question on which commentary is made is that to do with the time taken to decrypt computer files. The time that will be taken to decrypt a file or set of files is unpredictable. If material concerned with the encrypted material (keys, plain text, implementation details showing poor implementation) is found, the decryption times will be of the order of a few minutes in most cases. Historically, as stated by Dr Sommer (paras 14 to 17) decryption processes have worked in most cases for these reasons and in reasonable times (hours at most). What is unclear is whether these times are increasing and the number of cases for which decryption proves impossible is also increasing. I support Dr Sommer in his suggestion that these facts are gleaned from relevant witnesses. (para 17).

4. What is clear from the knowledge I have is that the use of encryption processes to protect information on hard disks is becoming more available and indeed is being encouraged for legitimate law abiding users in order to protect themselves from identity theft, spyware and phishing attacks. (Cf http://www.getsafeonline.org/nqcontent.cfm?a_id=1104 published by the Central Sponsor for Information Assurance within the Cabinet Office.)

5. Thus I do not agree with Dr Sommer's assertion made in paragraph 15 that the "use of encryption . . . on a hard disk without reason . . . are grounds for suspicion and applications for extended detention". If encryption of material on hard disks becomes the norm as is suggested by Cabinet Office, then it could be seen as necessary for us all to carry justification of doing so. This is tantamount to carrying justification for having on us the keys to our houses and cars, they being the means of protection of our physical assets as encryption keys are the means to protect our information assets. This is unlikely.

6. Therefore detection of the presence of the use of encryption will no longer be an indicator of possible malfeasance by itself. Indeed were it to be so, it is likely a rapidly increasing number of legitimate users would be suspected of malfeasance. Furthermore if the use of encryption for legitimate reasons grows as the Cabinet Office, in my view rightly, asserts is desirable, then law enforcement agencies, in the absence of any other indicators of suspicion, will need to decrypt that material to find evidence of possible malfeasance. This tension in Government policy between law enforcement and supporting secure business practices has existed for many years but is only now, due to technological advances, becoming significant. Looking first for other suspicious indicators to justify subsequent decryption may be a more profitable route under these circumstances.

7. The case that is made by Assistant Commissioner Andy Hayman for extended detention to allow a greater probability of decryption of computer files then seems to me to rest on two factors; one that the decryption process is more likely to provide significantly more evidence in 90 days than 30 and two on the likelihood that encrypted material hides suspicious activity in the first place. It is my view that if decryption works at all it will work in hours, and if it does not work in that time then the unpredictability of decryption processes based on brute force techniques (cf Peter Sommer para 16 last bullet with which I agree) is at best a weak justification for an increase in detention time. Without the statistics for decryption times, resources available and numbers of concurrent cases it is not possible to work out the advantage of 90 days over 30 days. The Committee may choose to enquire whether such statistics are available.

8. The second factor of encryption hiding suspicious activity as a justification for extension seems to me to be even more tenuous. It is more likely that other evidence would make the case for detention in the first place and that encryption is included as a secondary factor. If the use of encryption for legitimate purposes becomes more widespread using its existence on storage media as a prima facie case seems to me to be ill founded.

9. The second question on which my opinion was sought is the length of time needed to obtain and analyse data from mobile phones. The question breaks into a number of parts (1) the nature of the data, calling information (traffic analysis) or content (see Peter Sommer paras 22 to 24), (2) the means by which it is "obtained" and (3) the depth to which it is analysed. These will be treated in turn.

10. One of the factors involved in determining the time taken to obtain the requisite data of any type is how much "metadata" is available to help the "finding process". Examples might include number called, number calling, location, time etc. It is to be noted that in 2004 the usage of mobile phones in UK was 62 billion minutes per year (<http://www.mobilemastinfo.com/information/history.htm>)

11. The elapsed time for the finding process in this volume of data depends critically on reducing the "search volume" with prior "metadata" and on the resources (computers, networks and advanced software) allocated to this process by the owners (strictly collectors) of the data, that is the mobile operators.

12. It will also depend upon how many operators are involved and what jurisdictions they are in (this influences how quickly they can start and what authorities they need to do so).

13. The nature of the data requested will also affect how long it takes to acquire it; traffic flow data is distributed throughout the systems of the operators concerned and may take some time to acquire, but is not seen as a major invasion of privacy by end users so collation of it could start as soon as the metadata to support the finding process is assembled; content on the other hand will probably only reside in the systems of the two operators with which the end users have accounts; but content of a call is regarded as sensitive by end users and hence warrants may be necessary for access depending upon the jurisdiction in which it is stored.

14. It is clear therefore that predicting the time to obtain the data of whatever type is not possible. What is clear is that the volume of data within which the desired information resides is increasing rapidly and that the complexity of the data structures is increasing also. Without improvements in finding techniques it is clear that finding times will go up also. Hence there appears to be a reasonable case for increasing detention times whilst this process is completed. However, the Committee might like to enquire whether the Home Office is exploiting current research aimed at finding new and much faster ways of finding information in large volumes of data as an alternative to the need for increased detention times. (eg Exploitation of AKT: www.aktors.org/akt/objectives)

15. The time taken for analysis will depend upon how many staff with the requisite expertise and experience are allocated to any given case. It is impossible to predict how long this element of the overall process will take, but it is clear that as the complexity of material goes up so will the time for analysis; again, development of advanced tools and their widespread use would ameliorate the situation to some extent, but this also depends upon trained individuals in some considerable numbers being available.

16. The issues raised by Peter Sommer in para 28 of his submission are also particularly important. Most telecommunications systems and data communications systems will converge on to one global infrastructure in the next few years. The separation of what is content and what is traffic information will (and is already) becoming very difficult. This has legal as well as technical implications. Without global agreements on all aspects of law enforcement, use of intercepted material obtained by whatever means will become more and more problematic. The case for extended detention periods based on technology innovation outstripping legal instruments will then look ill founded, unless technology in support of law enforcement is used effectively.

30 January 2006

22. Memorandum submitted by Daren Greener

EXECUTIVE SUMMARY

This report has been compiled following a request from the Parliamentary Office of Science and Technology for information in regard to issues affecting mobile phone evidence. It draws upon more than three years' experience of work specialising in forensic analysis of mobile phone evidence relied upon in criminal cases nationwide. During the past two years alone, I have undertaken work leading to some 50 reports and provided oral testimony in court on a number of occasions.

Chapter 1 provides an insight into the practices of telecommunications analysis with particular emphasis on that of mobile phone evidence and investigations. It highlights the reliance within such investigations on call data (phone billing usage records and cell-site information) held for limited periods of time by the mobile phone service providers.

Having highlighted the process of investigation and the obtainable outcomes, Chapter 2 then provides summary details of the existing availability of call records.

Chapter 3 outlines the implications this has for phone examination work. It also illustrates the benefits to be gained from being able to rely upon common extended minimum standards of call data recording by the mobile phone network providers and extension of the existing data retention periods for call data.

Finally, the arguments are summarised for the extension of existing data retention periods and the need to increase and standardise the supply of call records for all call events types.

1. MOBILE PHONE EVIDENCE

There are three main areas for the forensic analyst to review as follows:

1. Equipment Examinations—The retrieval and analysis of data stored on, or recoverable from the mobile phone equipment (Handset and SIM Card Subscriber Identity Module).
2. Call Billing Record Analysis—The analysis of call records to identify common associations and patterns of communications, cross-referencing with data from equipment examination, etc.
3. Cell-Site Analysis—Identifying the location and movements of mobile phones according to their historical call records.

To a greater or lesser extent, there is a requirement for data to be provided from the relevant network provider in all aspects of the work outlined above.

1.1 "Equipment examination"

This is the examination, data retrieval and capture of information saved within either the SIM (Subscriber Identity Module) card or mobile phone handset. There is a very wide range of mobile phone models in use and specifications vary greatly.

1.1.2 The data capacity of mobile phones continues to expand as new models come onto the market. Already many phones have the capability to store many hundreds of text messages, and thousands of stored telephone numbers. Certain phone models have removable storage cards that are used to store larger volumes of user data, these memory cards can be subjected to further processes to recover deleted data.

1.1.3 Data sources available within a mobile phone include, contact and associate information, contents of text messages (including recovery of text messages deleted from the SIM card), video data, photo images either taken or received by the phone, stored audio voice recordings, calendar and appointments data.

1.1.4 Data extracted from the phone requires validation and verification. This includes validation of the time and date held by the phone and incorporated into some records. In the case of text messages, it is possible to falsify a sender's detail and also to alter the content after receipt. Techniques are employed by the analyst to identify suspect data.

1.1.5 Analysis of the data information in relation to phone numbers (call data, address book entries) obtained from a handset may require follow-up investigation to gather subscriber details (where maintained) or call records belonging to the phone numbers obtained. These aspects require appropriate requests to the relevant network operators for call records data, subject to the data retention period.

1.2 *Call Billing Record Analysis*

Call billing records provide detail for all chargeable transactions.

1.2.1 The process of call billing involves the examination of a person(s) phone call records to identify one or more of the following:

- To identify other third-parties who have made communication with the target phone number being examined (the creation of "friendship trees").
- To understand what communication has taken place with other third parties, including the duration and frequency of calls or text messages.
- To identify patterns of communication behaviour and deviations from those patterns.
- To demonstrate the use/interaction or transfer of particular mobile phone handsets when billing records include the handsets IMEI identifier.

1.2.2 Due to the prevalence of unregistered SIM cards and ease in transfer of phone ownership, subscriber details may not be available or applicable. Therefore, further investigations have then to be made on the phone numbers found within the target records in an attempt to positively identify phone ownership/association. This process can significantly increase the time expended on investigation.

1.2.3 During call billing analysis other parties may be positively identified. This may call for similar analysis on other identified numbers. At that stage, requests for the billing data have to be made and the process can reiterate many times. Each stage can be time consuming and that time expending will be reflected in the amount (time span) of call billing remaining in accordance with existing data retention.

1.2.4 For example a suspect telephone number is identified five months after an alleged incident. At that stage, based on 12 months' retention there is seven months' historical call data remaining leading up to the incident date.

1.2.4.1 The call records/phone equipment are examined and analysed and the process takes a further month. From the investigation five other telephone numbers are identified all on varying networks. At this stage there is six months of historical call data from the date of incident. However there is now no record of text message interaction for three of the phones because this data is only held for six months by the relevant network operator.

1.2.4.2 The analysis of these other records shows that there was significant interaction between these five phones and those of two others starting three months before the actual incident date. The second process of analysis has taken a further two months to compile and analyse but it is now shown that seven individuals conspired three months before the incident date and the common link is via two other numbers now identified.

1.2.4.3 The call records of these other two phones are now required, the investigation has been ongoing for three months. The historical call records remaining can only provide one month of historical data for these two phones prior to the identified period of conspiracy.

1.2.4.4 If at that stage other numbers are identified from the earliest call data there will not be any historical data retained as the data retention period from the alleged incident has diminished as time on the investigation is expended.

1.2.4.5 The example above considers intelligence/evidence discovery well within the existing data retention period (ie 12 months "rolling" historical). However the reality can be that the whole investigation period may take many months or years.

1.3 *Cell-Site Analysis*

The process of cell-site analysis considers the approximate location and movements of a mobile phone based upon the historical call events. When a mobile phone makes, and in many cases receives, a call the relevant network operator will record the unique identifier of the cell-site or cell-site-sector that the call was routed to or from.

1.3.1 A network provider can supply historical call records that show the cell-site identity for each call event. However there is a variance in the level of detail supplied by network operators. For example in some cases it is possible to have both the identity of a cell-site that a call started from and also the identity of the cell-site that the call terminated on. Other providers only supply the start of call cell-site.

1.3.2 As with most forms of analysis, the more data available the greater the level of analysis that can be performed.

1.3.3 In the initial stages of cell-site analysis, the analyst will receive information in regard to the cell-sites that have served call events for particular mobile phones. The typical cell-site information supplied by a network operator will include the following:

- name of the site;
- postcode and/or address;
- easting and northing settings, (map co-ordinates of sites);
- number of cell-sectors;
- cell-sector identification numbers; and
- azimuth/bearing setting (direction in which antenna is facing in from true north).

1.3.4 Methodologies for cell-site analysis are not defined and as such may vary from analyst to analyst. However, I regard that certain principles exist in the performance of cell-site analysis and these are given below:

- Define the cell-site sector that served a call event (reliance on available data).
- Plot the position of that cell sector. (call mapping process).
- Understand the scale and scope of coverage from that sector (Prediction, Review Operator's Best Server Plots for incident dates, Field Measurement Surveys).
- Validate/verify the sector coverage according to documented settings. (Survey).
- Survey actual areas of interests and detect/define an order of service for cell-site coverage. (Spot Measurement Surveys).
- Plot the positions of other relevant cells according to the order of service. (Network Modeling).
- Consider other relevant issues such as local demographics and topology.
- Based on the results of the above make location and/or movement predictions where possible.

1.3.5 Cell-site changes can dramatically alter the footprint area of coverage provided from a particular cell-site or cell-site sector, altering the range (how far), width (how wide) and shape of each particular coverage area. The following provides a non-exhaustive list of the types of cell-site changes that can affect/alter the coverage area provide by a cell-site or cell-site sector:

- Changes to antenna type and antenna efficiency, gain levels.
- Changes to the physical positioning of antenna (lateral position changes).
- Changes to azimuth settings.
- Height changes.
- Vertical elevation changes, grazing angles (vertical polarisation).
- Power level changes.
- Power control changes.
- Channel frequency changes.
- Several other front-end changes that would affect the resulting coverage patterns.

1.3.6 When performing cell-site analysis after any notable time from the actual time that calls were made, it is important to understand what changes have taken place to the mobile phone network for a particular area. Whilst the network operators are often able to provide details of historical changes and planned maintenance (cell-site downtime), the level of detail is limited and often found to be incomplete or not available.

2. NETWORK PROVIDER DATA

2.1 In the UK the main network providers (data owners) are O₂, Orange, T-Mobile, 3Three (Hutchinson) and Vodafone. Virgin Mobile also generates and retains billing data, but its backbone network provision (actual cell-sites) is provided by T-Mobile.

2.2 These network operators record the details of the call events to and from a mobile phone. This data can include the identity of the cell-site or cell-site sector that a call was routed from/to.

2.3 At present there is a variance in both the level of data recorded by each operator and also in the length of time that data is retained.

Under current practices data is retained for no more than 12 months. However, variances can mean that historical call events including data for text message exchange may only be held for six months or less in the case of certain account types (ie contract, pre-pay, pay-as-u-go).

2.4 It should be noted that the actual content/prose of historic text messages is not recorded/provided by any of the providers. This data may on occasion be available when an identified request for such data is made within days of a particular transaction.

2.5 Each of the main network operators maintains a department to provide historical data or court liaison for law enforcement purposes. These departments supply historical call records and details of cell-site locations on a chargeable basis.

3. DATA REQUIREMENTS—STANDARDISATION OF CALL DATA

3.1 Standardisation on the level of historical data available from all the network operators would improve the quality of telecommunications evidence and reduce the overall time taken during investigation and analysis. At a minimum level the following should be provided regardless of account type.

3.1.1 Historical Call Billing records to detail the following:

- Phone numbers of other phones receiving or making calls/texts to and from the target phone.
- The date and time of the call events (connecting calls, diverts to voicemail or text messages).
- The duration of calls and the ringer/register (time to answer) duration for those calls.
- The IMEI handset identifier for all calls.

3.1.2 Cell-site call data to include:

- Start and End cell-site identifier for each call event and cell-site for text message dispatch or receipt. This to be provided for both the A end (caller) and B end (receiver) of each call event. Some operators provide this when both A and B end phones are registered to that particular network operator.
- Record of the “Timing slot and advance” issued for a particular call. This data is not currently provided by any operator within standard cell-site data. Its inclusion within records would assist the analyst in predicting if the call was made close to or far away from the epicentre of the cell-site and therefore increase the level of accuracy for predictions of call location.

3.1.3 For cell-site configuration data, the following is required in addition to the standard information (location and azimuth settings) currently provided:

- Height of antenna.
- Power output.
- Vertical polarisation (down tilt).

3.1.4 For historical changes to cell-sites the following data should be maintained and available on request:

- Changes to azimuth settings, height, power output and vertical polarisation.
- Changes to the mobile network in a given area, cell-sites commissioned or decommissioned.
- Record of cell-site down-time.

4. SUMMARY—DATA RETENTION REQUIREMENT

In any review of phone evidence and data retention the following factors should be considered.

4.1 Most people nowadays carry a mobile phone and are carried and used not only by perpetrators of crime and their associates, but also by victims and witnesses of crime. In many of the criminal cases on which I have been instructed to provide expert opinion on phone evidence, a large number of mobile phones have been involved.

4.2 The process of investigation takes several weeks or months depending upon the circumstance of crime/allegation. Furthermore, some time has passed since the incident under investigation took place before work is requested.

4.3 There is a variable time factor involved in all stages of the evidence identification, retrieval and analysis. From that examination further additional requests for call records may be required. Those records may then require separate analysis from which other numbers may be identified where once again further call records are required. An investigation can expand and may need to consider the historical movements and locations of other mobiles. There is a delay to each stage during which the data retention period is continually decreasing.

4.4 Under existing conditions data retention of mobile telecommunications data is at best 12 months with further restrictions applying to text message transfer details and in data relating to particular account types.

4.5 In a Utopian world it would be beneficial to have standardisation on the level of historical data that is provided. For cell-site analysis there is also a need for standardisation in the level of data being provided by the network operators and where possible an increase to fields of data recorded or made available.

4.6 There is a very strong need to increase and standardise the supply of call records for all call events types. Having regard to the time required to fully investigate and analyse such data, a minimum of two years' (24 months') data retention should be applied and this should be imposed for all inbound and outbound calls or text messages regardless of account types. An increase to a level of five-years' data retention should also be considered, treating call data similar to that of financial transactions for VAT purposes. Any increase to the existing data retention period would be beneficial to criminal investigations or matters of national security and especially when combined with standardisation in the level of details recorded.

4.7 The proposed upgrading of data retention may have implications on data storage requirements for the network providers. Increases in call data retention periods would be beneficial to the majority of criminal investigations and it is therefore perceived that there would be a significant increase in the requests of such data.

An anticipated increase in the revenue generation stream for network operators providing this historic data should be considered against the inevitable additional storage cost arguments forwarded by the network providers in response to proposals to extend existing data retention for call records.

4.8 The existing practises for data retention of call records is inadequate given the prevalence of mobile phones in society and the overall time for any investigation or information gathering periods.

4.9 Standardisation in the supply of call records together with a significant increase in the data retention period should be considered vital to British judicial system and to the interests of national security. Without these enhancements, evidence that may be gathered as a result of mobile phone usage is likely to be lost.

Appendix

OTHER ISSUES

In the realm of telecommunications evidence there are a number of other issues that require addressing. Examples of such are briefly summarised as follows:

- There is no control of unregistered SIM cards (mobile phone number) and the transfer of phone ownership.
- The so-called "Stolen Phone Database" is inadequate as it remains possible to reprogram IMEI identities and the database/operator systems cannot check against duplicate or invalid IMEI numbers.
- When performing mobile phone equipment examinations, certain constabularies within the UK can be shown to be using examination software that can be challenged on the forensic output produced.
- The development and deployment of the UMTS (3G Network) will severely limit the practise of cell-site analysis.

23. Memorandum submitted by the Metropolitan Police Service

The purpose of this report is to provide the answers and supporting documentation in response to the questions raised in the letter dated 20 March following the Home Affairs Select Committee visit to Paddington Police Station. A copy of the letter is attached at Appendix A [*not printed*].

1. What is the total number of police cells nationally that are suitable for holding terrorist suspects?

All of the county constabularies in England, Wales and Scotland have identified police stations within their respective force areas, where arrangements have been made for the detention of terrorist suspects when arrested as a result of a pre-planned operation. This is a total of about 80 police stations.

The attached document at Appendix B [*not printed*], prepared by the National Joint Unit (NJU), gives the location of all of the above police stations.

The secure suite at Paddington Green is the only "purpose-built" facility in England and Wales for terrorist-related detainees.

There is a Scottish Terrorist Detention Centre (STDC), which is a purpose-built facility (approximately 10 years old), located in a police office in Glasgow.

It should be noted that persons arrested under terrorist legislation may be legally detained at any police station that is "designated" under the Police and Criminal Evidence Act. For example, if a patrolling officer makes an arrest under terrorism legislation as a result of a call to suspicious activity, the suspect will be taken to the local designated police station.

2. *Please provide a typical application to a District Judge for an extension of pre-charge detention under the existing arrangements.*

Please see attached documents at Appendix C [*not printed*]. These are two examples of Schedule 8 Applications for warrants of further detention, drawn from the investigation into the July bombings. Also attached is a copy of the explanatory guide for the benefit of police officers [*not printed*] (this guide is presently being reviewed and modernised).

3. *Please provide an analysis of at least 10 recent terrorist investigations showing how many suspects in each inquiry were represented by the same solicitor or same firm.*

Attached at Appendix D [*not printed*] is a table showing the dates of the requested number of operations resulting in multiple detainees at the Paddington Green secure suite, and the firms of solicitors that represented the detainees.

4. *Please provide details of the cross-border case referred to by Lord Carlile in his answer to the Committee on 14 February.*

This case is “Operation ***”. The senior investigating officer was Mr Bert Swanson from Lothian and Borders Police. Mr Swanson, having retired as a police officer, is still employed by Lothian and Borders police, as a cold-case reviewer.

Also attached at Appendix E [*not printed*] is a copy of a leaflet, which has been produced, apparently by Arani and Co. The Committee became aware of the existence of this leaflet during their visit to Paddington and have specifically requested a copy.

April 2006
