House of Commons

Home Affairs Committee

Unauthorised tapping into or hacking of mobile communications

Thirteenth Report of Session 2010–12

1. This report is **strictly embargoed** and is not for broadcast or publication, in any form, before 05.00hrs, Wednesday 20 July 2011.

2. This report is issued under the condition that it should not be forwarded or copied to anyone else.

3. Under no circumstances should you distribute copies to anyone else or speak to the media before the publication time about the content of this report.

5. If these instructions are unclear in any way please contact Alex Paterson on 020 7219 1589 or email commonsmedia@parliament.uk

HC 907

House of Commons

Home Affairs Committee

Unauthorised tapping into or hacking of mobile communications

Thirteenth Report of Session 2010–12

Ordered by the House of Commons
to be printed 19 July 2011

HC 907
Published on 20 July 2011
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

The 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.

Current membership

Rt Hon Keith Vaz MP (*Labour, Leicester East*) (Chair)
Nicola Blackwood MP (*Conservative, Oxford West and Abingdon*)
James Clappison MP (*Conservative, Hertsmere*)
Michael Ellis MP (*Conservative, Northampton North*)
Lorraine Fullbrook MP (*Conservative, South Ribble*)
Dr Julian Huppert MP (*Liberal Democrat, Cambridge*)
Steve McCabe MP (*Labour, Birmingham Selly Oak*)
Rt Hon Alun Michael MP (*Labour & Co-operative, Cardiff South and Penarth*)
Bridget Phillipson MP (*Labour, Houghton and Sunderland South*)
Mark Reckless MP (*Conservative, Rochester and Strood*)
Mr David Winnick MP (*Labour, Walsall North*)

The following members were also members of the committee during the parliament.

Mr Aidan Burley MP (*Conservative, Cannock Chase*)
Mary Macleod MP (*Conservative, Brentford and Isleworth*)

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.

Publication

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 Elizabeth Flood (Clerk), Joanna Dodd (Second Clerk), Sarah Petit (Committee Specialist), Eleanor Scarnell (Inquiry Manager), Darren Hackett (Senior Committee Assistant), Sheryl Dinsdale (Committee Assistant), Victoria Butt (Committee Assistant), John Graddon (Committee Support Officer) and Alex Paterson (Select Committee Media Officer).

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.

Contents

Report

1 Introduction

Background

1. In 2005-06, the Metropolitan Police investigated claims that a private investigator, Mr Glenn Mulcaire, had been employed by News International to hack into the Voicemail accounts of certain prominent people, including members of the Royal Household in November 2005, in particular to obtain information on them. This case led to the prosecution and subsequent imprisonment of Mr Mulcaire and Mr Clive Goodman, the royal correspondent for the *News of the World*. The charges brought against Messrs Mulcaire and Goodman cited a limited number of people whose phones were alleged to have been hacked. However, papers taken from Mr Mulcaire in the course of the investigation indicated that journalists —not necessarily all from the same newspaper — had asked him to obtain information on a number of other people: it was not always clear who the subjects of the inquiries were (a number were identified only by initials or a forename), nor whether the request involved hacking or some other means of obtaining information.

2. In 2006 the Information Commissioner, who is responsible for overseeing the UK's data protection laws, published two reports, *What price privacy?* and *What price privacy now?* which gave details of investigations conducted by his office and the police into "a widespread and organised undercover market in confidential personal information." In one major case, known as Operation Motorman, the police and Information Commissioner's Office found evidence that 305 journalists working for a range of newspapers had used a variety of techniques to obtain personal information for their stories (more details are provided in Appendix A). Some of the information could have been obtained only illegally; other pieces of information could be obtained legally (e.g. addresses via voter registration records) but this would have been very time-consuming

and the prices paid to the private investigators obtaining the evidence were too low for such onerous work.[1]

3. In 2009 it became known that one person who considered he had been a victim of hacking by Mr Mulcaire at the instigation of a *News of the World* journalist had launched a civil case against that paper's owners, News International and, it was reported, had received a large amount in damages in settlement whilst agreeing to be bound by a confidentiality clause. The successful litigant was Mr Gordon Taylor of the Professional Footballers Association. The media noted at the time that he was unlikely to have been of interest to the royal correspondent, so it was suspected that other News International journalists or editors might have been involved with similar activities.

4. The names of other successful litigants gradually leaked out. Over the next few months, a growing number of alleged victims of hacking brought civil actions against News International or sought judicial reviews of the handling of the original case by the police, and demanded that the police release documents seized from Mr Mulcaire relevant to their cases.

5. At the same time, the *Guardian* newspaper was continuing to investigate the relationship between Mr Mulcaire and News International journalists, focusing in particular on claims by some former journalists that practices like hacking were widespread in the *News of the World*. Because of the concerns raised by the new allegations, on 9 July 2009 the Commissioner of the Metropolitan Police asked Assistant Commissioner John Yates, QPM, to look into the case. We deal with both the 2005–06 investigation and Mr Yates's role in 2009 later in this report.

6. We were aware that our sister committee, the Culture, Media and Sport Committee, had had a longstanding interest in the ethics of reporting and reporting methods, and were repeatedly taking evidence on this issue. Whilst the role of the media was clearly part of that Committee's remit, questions were being asked about the response of the police to the

1 The reports were published respectively in May and December 2006, and may be found at www.ico.gov.uk. The quotation is taken from *What price privacy?,* paragraph 1.7.

original allegations in 2005–06, and there appeared to be some confusion about the interpretation of the legislation governing hacking which had the effect of making it unclear who precisely might be considered a victim of that crime. Accordingly, early in September 2010, we launched an inquiry into 'Unauthorised tapping into or hacking of mobile communications', with the following terms of reference:

- The definition of the offences relating to unauthorised tapping or hacking in the Regulation of Investigatory Powers Act, and the ease of prosecuting such offences;
- The police response to such offences, especially the treatment of those whose communications have been intercepted; and
- What the police are doing to control such offences.

During the course of the inquiry, it became clear that it was necessary to examine other aspects too:

- The scope of the police inquiry in 2005–07;
- The role of the mobile phone companies in providing security information to their customers and in relation to those whose phones may have been hacked into; and
- The relationship between the police and the media.

Our focus has remained on the police, the prosecutors, the victims and the legislation: in this Report we do not attempt to reach any conclusions and recommendations about the actions of specific newspapers or individual journalists.

7. We had invited Mr Yates to give oral evidence to us on 7 September 2010 as the head of the Metropolitan Police's Specialist Operations Unit on the two main areas dealt with by his unit: Royal and diplomatic protection and Counter-terrorism. We took the opportunity of asking him about the 2005–06 investigation and subsequent developments. This evidence has already been published.[2] We later took oral evidence again from Mr Yates, Mr Chris Bryant MP, the Director of Public Prosecutions, the Information Commissioner, representatives of three mobile phone companies (Telefonica O2, Vodafone, and the

2 As Home Affairs Committee, *Specialist Operations, Oral evidence, 7 September 2010*

Orange UK and T-Mobile UK joint venture, Everything Everywhere), Lord Blair of Boughton QPM, Mr Peter Clarke CVO, OBE, QPM, and Mr Andy Hayman CBE, QPM, (the two senior police officers who oversaw the 2005–06 investigation) and Deputy Assistant Commissioner Sue Akers, QPM, who is in charge of the current investigation. In our final session, we took evidence from Sir Paul Stephenson, Metropolitan Police Commissioner, Mr Dick Fedorcio, the Director of Public Affairs and Internal Communication at the Metropolitan Police Service, Lord MacDonald of River Glaven QC and Mr Mark Lewis, solicitor. We received several pieces of written evidence, all of which have been published on our website and are printed with this Report, and we have corresponded on a number of occasions with our oral witnesses, and with Ms Rebekah Brooks, then Chief Executive Officer of News International, Assistant Commissioner Cressida Dick, the National Policing Improvement Agency, the Serious Organised Crime Agency and HM Chief Inspector of Constabulary (the last four on the question of rules governing the payment of police by the media and others). We would like to express our gratitude to all who have given evidence to us, and in particular to those who have repeatedly responded to our further questions as our inquiry developed.

Subsequent developments

8. Since we opened our inquiry, the following events have occurred. On 12 November 2010, after interviewing the former reporter the late Mr Sean Hoare and others, the Metropolitan Police said that it had uncovered further material about hacking and passed the file of evidence to the Crown Prosecution Service to consider whether there was strong enough evidence to bring criminal charges. The Head of the CPS Special Crime Division, Mr Simon Clements, decided on 10 December 2010 that there was no admissible evidence to support further criminal charges, as the witnesses interviewed had refused to comment, denied any knowledge of wrongdoing or had provided unhelpful statements.

9. On 5 January 2011, however, the *News of the World* suspended Mr Ian Edmondson from his post as assistant editor (news) following allegations that he was implicated in the hacking of Sienna Miller's phone—Ms Miller's lawyers had found notes among the documents released by the police indicating that Mr Mulcaire might have hacked into her

phone on instructions from Mr Edmondson. The Metropolitan Police then wrote to News International requesting any new material it might have following the suspension. Acting Commissioner Tim Godwin opened a new inquiry, led by Deputy Assistant Commissioner Sue Akers and codenamed 'Operation Weeting'.

10. The media continued to pursue the story of the extent of 'hacking' by people employed by News International in the period from about 2003–06, and (subsequently) both before and after this period. On 5 April 2011, Mr Edmondson and Mr Neville Thurlbeck, the chief reporter for *News of the World*, were arrested on suspicion of conspiring to intercept communications (contrary to Section1(1) of the Criminal Law Act 1977) and unlawful interception of voicemail messages (contrary to Section 1 of the Regulation of Investigatory Powers Act 2000). They were later released without charge on police bail until September 2011. Further arrests (including that of a royal reporter with the Press Association) have been made since then. The new police inquiry under DAC Sue Akers continues.

11. The story took a new turn when the media reported allegations that Mr Mulcaire may have hacked into the phone of Milly Dowler, a 13-year old murdered in 2002, and the phones of her family and friends. It was also alleged that the phones of the families of the Soham murder victims had been hacked into in 2002 and that the same had happened to the phones of victims of the 7th July bombings in London in 2005. An emergency debate in the House of Commons on 6 July 2011 showed strong support for a public inquiry into the phone hacking at the *News of the World* and the conduct of the Metropolitan Police between 2006 and 2011.[3] The Prime Minister indicated that the Government agreed in principle to a public inquiry in two stages that would consider the conduct of the media generally and the history of the police investigations from 2005 onwards. Subsequently, the terms of reference have been announced, as has the fact that Lord Justice Leveson is to head the inquiry. It had initially been argued that a public inquiry or judge-led inquiry could only start work once police investigations and any consequent prosecutions had been brought to a conclusion. MPs had argued strongly that the Inquiry should be established straight away so that the judge leading it could immediately secure any evidence that might

3 HC Deb, 6 July 2011, col 1543 onwards

otherwise be destroyed (although this would be a criminal offence), and so that a start could be made on issues not pertinent to ongoing investigations and prosecution. There was a clear understanding on all sides that nothing should be done that might prejudice the current police investigations.The timing and timescale of these inquiries remain to be determined. We welcome the fact that the Prime Minister consulted us on the terms of reference for this inquiry.

Involvement of police witnesses in various inquiries

12. It may be useful here to provide a brief indication of which of our witnesses (police officers and prosecutors) were involved in the various police inquiries and when. At the time of the first investigation, Mr Peter Clarke was Deputy Assistant Commissioner with the Specialist Operations Directorate (which had been formed from the merger of the Counter-Terrorist Command and the Royal and Diplomatic Protection group). Mr Clarke was the most senior officer with day-to-day responsibility for the 2005–06 police investigation into hacking. Mr Andy Hayman was at that time Assistant Commissioner for Specialist Operations, and Mr Clarke's superior officer. Lord Blair of Boughton, then Sir Ian Blair, was Commissioner of the Metropolitan Police between 2005 and 2008. Mr Hayman resigned from the service in December 2007 and Mr Clarke retired in February 2008, so neither was still in post at the time when further allegations appeared to be emerging in the press in 2009. Lord Macdonald of River Glaven, QC, then Sir Ken Macdonald, was Director of Public Prosecutions between 2003 and 2008.

13. By July 2009, the Commissioner of Police of the Metropolis was Sir Paul Stephenson QPM, and Mr John Yates was Assistant Commissioner for Specialist Operations, having replaced Mr Hayman's successor (Bob Quick) in April 2009. Sir Paul asked Mr Yates to look into the stories emerging in *The Guardian* and subsequently the *New York Times* alleging that the hacking of mobile phones was a widespread problem not confined to those investigated and prosecuted in 2006–07. Mr Keir Starmer, QC, had succeeded Sir Ken Macdonald as Director of Public Prosecutions. The members of the Crown Prosecution Service giving advice directly to the police at this time were not the same people as had advised the police in 2006–07.

14. In January 2010, the Metropolitan Police decided to open a new investigation. DAC Sue Akers was appointed to head the investigation, which is known as Operation Weeting. Subsequently, DAC Akers was also to head the investigation into allegations of payments by News International journalists to officers of the Metropolitan Police.

Table 1: Timeline of events

Date	Events	Police investigation	Commissioner
January 2003	Rebekah Brooks and Andy Coulson give evidence to the Culture, Media and Sport Committee. Brooks admits to paying police officers for stories.		
November 2005	The News of the World publishes a story about Prince William's knee injury. This prompts a complaint to police that voicemail messages of royal officials have been intercepted.	Investigation led by (then) Deputy Assistant Commissioner Peter Clarke	Commissioner Sir Ian Blair
August 2006	Police arrest Clive Goodman (royal editor, News of the World) and Glenn Mulcaire (private detective).		
January 2007	Clive Goodman and Glenn Mulcaire convicted of conspiring to intercept communications. Goodman is sentenced to 4 months in prison, Mulcaire is sentenced to 6 months.		
March 2007	Les Hinton gives evidence to Culture, Media and Sport Committee. He tells the Committee that an internal investigation found no evidence of widespread hacking at News of the World.		
May 2007	The Press Complaints Commission, the newspaper regulation watchdog, published a report on hacking but said it found no evidence of wrongdoing at the News of the World. Harbottle and Lewis, News International's lawyers,		

	reviewed internal emails between Mr Coulson and executives and found no evidence they were aware of Goodman's actions.		
July 2009	The Guardian Newspaper publishes an article which details over £1 million in payments made by News International to settle court cases which focus on journalists alleged involvement in hacking. Scotland Yard announces that it has reviewed the evidence and no further investigation is required. The Crown Prosecution Service announces an urgent review of material provided by the police in 2006. Colin Myler and Andy Coulson give evidence to Culture, Media and Sport Committee	Review led by Assistant Commissioner John Yates	Commissioner Sir Paul Stephenson
November 2009	The Press Complaints Commission publishes a second report on News of the World. It finds no new evidence to suggest that anyone at News of the World other than Mulcaire and Goodman was involved in phone hacking.		
February 2010	Culture, Media and Sport Committee publishes report on Press standards, privacy and libel which suggests that it is inconceivable that senior management at the paper were unaware of widespread hacking.		
September 2010	New York Times publishes an article claiming that Andy Coulson was aware that his staff at News of the World were illegally hacking voicemail. It also questioned whether the Met police were fully committed to the original investigation. The article prompts further calls for a new inquiry.		

December 2010	The Crown Prosecution Service announces that no further charges will be brought over the News of the World phone hacking scandal because witnesses refused to co-operate with police.		
January 2011	Met police open a new investigation into allegations of phone hacking.	Operation Weeting, led by Deputy Assistant Commissioner Sue Akers	Acting Comissioner Tim Godwin
June 2011	300 emails retrieved from law firm Harbottle & Lewis handed to Metropolitan police by News International.		
July 2011	Met police announce operation Elveden to look at payments made to police by News International. Operation Elveden is a subset of Operation Weeting. Sir Paul Stephenson and John Yates resign.	Operation Elveden, led by Deputy Assistant Commissioner Sue Akers	Commissioner Sir Paul Stephenson

2 The legislation covering interception of electronic communications

15. When Mr Clarke and Mr Hayman came to investigate the allegations of interference with the voicemails of members of the Royal Household in November 2005, the police were faced with various pieces of legislation that might be used against the perpetrators, each of which had advantages and disadvantages. The one on which, on advice from the Crown Prosecution Service ('CPS'), they chose to focus was section 1 of the Regulation of Investigatory Powers Act 2000. However, sections of the Data Protection Act 1999 and the Computer Misuse Act 1990 were also relevant.

16. We discuss these latter two Acts first and explain why the police and the CPS were disinclined to use them, before going on to set out the difficulties surrounding section 1 of the Regulation of Investigatory Powers Act.

Computer Misuse Act and Data Protection Act

17. The offence under section 1 of the Computer Misuse Act is committed where a person knowingly 'causes a computer to perform any function' with intent to secure unauthorised access to any program or data held in any computer, or to enable any such access to be secured. There has to be some interaction with the computer, so that merely reading confidential data displayed on a screen or reading the printed output from the computer would not constitute the offence. On the other hand, it can be argued that that using the owner's PIN number or password without his authority to access his e-mails or voicemails would fall within the scope of the offence, as it would cause the computer to perform a function.

18. Until 2008, the offence under s.1 of the 1990 Act was triable summarily, with a maximum penalty of only six months' imprisonment. This was therefore the situation during the first investigation into hacking in 2005–06. The offence is now[4] also triable on

4 See section 35(3) Police and Justice Act 2006.

indictment with a maximum penalty of two years' imprisonment, the same mode of trial and penalty as the interception offence under the Regulation of Investigatory Powers Act.

19. The Data Protection Act 1998 creates a number of offences, but the most relevant is the offence of unlawful obtaining of personal data. Section 55 of the 1998 Act makes it an offence knowingly or recklessly to obtain or disclose personal data without the consent of the data controller. The offence may be tried either summarily or on indictment. Section 77 of the Criminal Justice and Immigration Act 2008 confers an order-making power to provide for the imposition of a sentence of imprisonment, but this has not yet been brought into effect and currently, the penalty is limited to a fine.

20. It is very difficult to imagine a voicemail or other personal message which did not contain some personal data of either the sender or the intended recipient. However, section 55(2) provides for a number of defences which conceivable might inhibit a successful prosecution for 'hacking'. Of most direct relevance to this case, it is a defence to show that the obtaining or disclosing was justified as being in the public interest (s.55(2)(d)). This defence has been prospectively broadened by a new s.55(2)(ca)[5] which makes it a defence to show that the person acted with a view to the publication by any person of any journalistic, literary or artistic material, and in the reasonable belief that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest. Journalists inquiring into public figures might seek to rely on the new defence but would need to show that they were acting in the public interest. The defence is unlikely to apply at all in relation to the alleged tampering with the voicemails of essentially private individuals unwittingly brought to public attention through their connection with victims of crime or with service personnel killed in battle; but the police and prosecutors claim not to have been aware of these cases at the time because they had not fully reviewed the other 11,000 pages from the Mulcaire case.

21. The current Director of Public Prosecutions, Mr Keir Stamer QC, in a letter to us recognised the disadvantages of using these two pieces of legislation in the circumstances

5 Inserted by s.78 Criminal Justice and Immigration Act 2008 not yet in force.

of the time, saying: "So far, prosecutions have (rightly in my view) been brought under the Regulation of Investigatory Powers Act 2000 (RIPA), but, depending on the circumstances and available evidence, offences under the Computer Misuse Act 1990 and/or the Data Protection Act 1998 might also fall to be considered in on-going or future investigations."[6]

Regulation of Investigatory Powers Act

Section 1 (Unlawful interception) of the Regulation of Investigatory Powers Act says:

> (1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of—
>
> (a)a public postal service; or
>
> (b)a public telecommunication system.
>
> (2) It shall be an offence for a person—
>
> (a)intentionally and without lawful authority, and
>
> (b)otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection,
>
> to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system.
>
> .....
>
> (7) A person who is guilty of an offence under subsection (1) or (2) shall be liable—
>
> (a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;
>
> (b) on summary conviction, to a fine not exceeding the statutory maximum.

Section 2 (Meaning and location of "interception" etc.)

[Subsection (1)defines "postal service" , "private telecommunication system", "public postal service", "public telecommunications service", "public telecommunication system", "telecommunications service" and "telecommunication system".]

(2) For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a

telecommunication system if, and only if, he—

(a) so modifies or interferes with the system, or its operation,

(b) so monitors transmissions made by means of the system, or

(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

.....

(7) For the purposes of this section the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.

(8) For the purposes of this section the cases in which any contents of a communication are to be taken to be made available to a person while being transmitted shall include any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently.

.....

22. The offence under Regulation of Investigatory Powers Act 2000 section 1 is committed by a person who (intentionally and without lawful authority) intercepts any communication "in the course of transmission" by a telecommunications system. The Director of Public Prosecutions told us: "Once the communication can no longer be said to be in the course of transmission by the means of the 'system' in question, then no interception offence is possible" and added: "Taking the ordinary meaning of those expressions one would expect the transmission of a communication to occur between the moment of introduction of the communication into the system by the sender and the moment of its delivery to, or receipt by, the addressee."

23. That appears to have been the basis on which the Crown Prosecution Service advised the police in 2005-06. It was also the very clear view of the CPS in July 2009 when it gave written evidence to the Culture, Media and Sport Committee and stated:

> THE LAW
>
> To prove the criminal offence of interception the prosecution must prove that the actual message was intercepted prior to it being accessed by the intended recipient.

24. However, Section 2(2) has to be read in conjunction with section 2(8) which provides that 'in the course of transmission' includes "any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently". Whilst it is clear that any stored message not yet received and heard or read may be considered still "being transmitted", what about messages already received and heard or read but left stored in the system? Again, as the Director of Public Prosecutions put it:

> The difficulty of interpretation is this: Does the provision mean that the period of storage referred to comes to an end on first access or collection by the intended recipient, or does it continue beyond such first access for so long as the system is used to store the communication in a manner which enables the (intended) recipient to have subsequent, or even repeated, access to it?

25. One of the roles of the courts is to clarify the construction of statute where necessary. For reasons that are described below, however, as yet no court has been asked to consider this issue.

26. We have gone into detail in relation to this question because the interpretation of these sections of the Regulation of Investigatory Powers Act has formed a major source of contention in respect of the definition of who has been a 'victim' of hacking and the likelihood of achieving successful prosecutions, influenced the conduct of the 2005–06 police investigation and the subsequent approach of the police to hacking, and was the focus of much of the disagreement among our witnesses as to what ought to have been done.

Impact of the interpretation of the legislation on the police investigations

27. Considerable argument before the Committee has focused on the advice on the interpretation of RIPA given by the Crown Prosecution Service to the police in 2005–07, whether the police correctly understood the advice, and whether the advice has changed subsequently.

28. In the course of his oral evidence to us in September 2010, Assistant Commissioner Yates was asked about the 91 people whose PIN numbers were allegedly listed in Mr Mulcaire's papers: the Chair referred to these people as 'victims' of hacking, and Mr Yates replied:

> "Victims of hacking" is taking it a bit far because hacking is defined in a very prescriptive way by the Regulation of Investigatory Powers Act and it's very, very prescriptive and it's very difficult to prove. We've said that before and I think probably people in this room are aware of that. It is very, very difficult to prove. There are very few offences that we are able to actually prove that have been hacked. That is, intercepting the voicemail prior to the owner of that voicemail intercepting it him or herself.[7]
>
> ***Chairman:*** But there are 91 PIN numbers, is that right?
>
> ***Mr Yates:*** There is a range of people and the figures vary between 91 and 120. We took steps last year, as I indicated last year, to say that even if there is the remotest possibility that someone may have been hacked, let's look and see if there is another category. Bearing in mind that we'd already had a successful prosecution and two people have gone to jail, we wouldn't normally do that, but because of the degree of concern I said we were to be extra cautious here and make sure we have established whether there is a possibility—and we put some criteria around that, which I won't bore you with—they have been hacked. That is where that figure comes from. It is out of a spirit of abundance of caution to make sure that we were ensuring that those who may have been hacked were contacted by us.[8]

He added: "We can only prove a crime against a very small number of people and that number is about 10 to 12 people. That is very few people."[9]

7 Q 5, in evidence published as *Specialist Operations,* 7 September 2011

8 Q 5, in evidence published as *Specialist Operations,* 7 September 2011

9 Q 9

29. This interpretation followed the approach taken by the police in 2005–07 on the basis of their understanding of the advice being given to them by the Crown Prosecution Service. The current Director of Public Prosecutions, Mr Keir Starmer, noted:

> In 2009, I gave written evidence to the Culture, Media and Sport Committee. In that evidence I set out the approach that had been taken to section 1(1) of RIPA in the prosecution of Clive Goodman and Glen Mulcaire, namely that to prove the criminal offence of interception the prosecution must prove that the actual message was intercepted prior to it being accessed by the intended recipient. I also set out the reasons why David Perry QC had approached the case on that basis at the time.

He went on to point out, however, that no distinction had been made in the terms of the charges against Messrs Mulcaire and Goodman between messages that had been accessed by the intended recipient and those that had not, and neither the prosecution nor the defence had raised this issue during the hearing, not least because both defendants in 2007 pleaded guilty. Therefore the judge was not required to make any ruling on the legal definition of any aspect of RIPA.[10]

30. Unfortunately, the construction of the statute, the interpretation of the CPS's advice in 2005–07 and the interpretation of evidence given to both us and our sister committee, the Culture Media and Sport Committee, all became the subject of dispute between Mr Yates, Mr Starmer and Mr Chris Bryant MP, with allegations of selective quotation and implications of deliberate misunderstanding of positions, and even of misleading the Committees, being made.[11] None of the participants had been present at the discussions of the cases of Messrs Mulcaire and Goodman, and all were relying on the recollections of those who were present and who could be asked for advice and the information supplied in any remaining documents, many of which had been drafted in the light of oral discussions and often to record a decision or position rather than to set out in detail every possible ramification of the discussions.

31. Whilst it is now impossible to know the exact course of the discussions between the police and the CPS at the time, Mr Peter Clarke, the witness who has closest to the original investigation as the senior officer in charge, made it clear to us that he understood the legal

10 Letter of 29 October 2010

11 The dispute started with an Adjournment debate in the House of Commons initiated by Mr Chris Bryant MP on 10 March 2010 (HC Deb, 10 March 2010), continued through the letter columns of the *Guardian* during the next few days, and then each of the protagonists was enabled to give his views to Committees of the House, Mr Yates to the Culture, Media and Sport Committee on 24 March, Mr Bryant and Mr Yates to us on 29 March, and the Director of Public Prosecutions to us on 5 April.

advice to be that they should proceed on a narrow construction of the statute. That is, that they should assume they could prosecute successfully only if they could prove that someone had accessed a voicemail message without authorisation before the intended recipient had heard it. The police were able to gather enough evidence to support this in one case involving Messrs Mulcaire and Goodman, and they were able to link five further cases to Mr Mulcaire on the basis of similarity of method, as Mr Yates described them to our sister committee, "inferential" cases.[12] As already stated, the two men pleaded guilty to all counts so the robustness of the inferential cases was never tested.

32. The National Police Improvement Agency (NPIA) provides advice to the police on their own operations. Ian Snelling, Covert Advice Team Manager in the NPIA Specialist Operation Centre confirmed that their advice to police, which had been 'essentially the same' since 2003, was as follows.

> Ultimately it will be a matter for the courts to decide whether a stored communication, which has already been accessed, is capable of interception but until such time it remains my view that, on a strict interpretation of the law, the course of transmission of a communication, including those communications which are stored on the servers of the CSP such as voicemail messages, ends at the point at which the data leaves the telecommunication system by means of which it is being (or has been) transmitted and is no longer accessible, and not simply when the message has been listened to. Accessing such voicemails could therefore amount to a criminal interception of a communication, as well as a civil wrong, and should therefore be conducted with the appropriate consents and/or lawful authority under e.g. RIPA s1(5)(c) or s3.[13]

33. In a letter to us dated 24 March 2011, Mr Yates cited a number of examples where the CPS in 2006 appeared to have taken a narrow interpretation of the offence. According to Mr Yates, this remained the police's understanding of how section 1 of RIPA should be interpreted until October 2010 when, in the context of the consideration of whether new evidence on the hacking issue was emerging, the new Director of Public Prosecutions addressed the construction of section 1. In his letter of 29 October 2010 to us, he stated:

> The role of the CPS is to advise the police on investigation and to bring prosecutions where it is appropriate to do so. In view of this, as I am sure you will appreciate, I

12 Q 454

13 Letter from Ian Snelling, NPIA, to Dr Julian Huppert

> need to take care not to appear to give a definitive statement of the law. For that reason, I will confine myself to explaining the legal approach that was taken in the prosecution of Clive Goodman and Glenn Mulcaire in 2006; and then indicate the general approach that I intend to take to on-going investigations and future investigations.
>
> ... I have given very careful thought to the approach that should be taken in relation to on-going investigations and future investigations.
>
> Since the provisions of RIPA in issue are untested and a court in any future case could take one of two interpretations, there are obvious difficulties for investigators and prosecutors. However, in my view, a robust attitude needs to be taken to any unauthorised interception and investigations should not be inhibited by a narrow approach to the provisions in issue. The approach I intend to take is therefore to advise the police and CPS prosecutors to proceed on the assumption that a court might adopt a wide interpretation of sections 1 and 2 of RIPA. In other words, my advice to the police and to CPS prosecutors will be to assume that the provisions of RIPA mean that an offence may be committed if a communication is intercepted or looked into after it has been accessed by the intended recipient and for so long as the system in question is used to store the communication in a manner which enables the (intended) recipient to have subsequent, or even repeated, access to it.

34. **We have been frustrated by the confusion which has arisen from the evidence given by the CPS to us and our sister Committee. It is difficult to understand what advice was given to whom, when. Only on the last day on which we took evidence did it become clear that there had been a significant conversation between the Director of Public Prosecutions and Assistant Commissioner Yates regarding the mention in the Mulcaire papers of the name Neville and whether this and Mr Mulcaire's contract with News International were a sufficient basis on which to re-open the investigation. The fact that the CPS decided it was not, does not in any way exonerate the police from their actions during the inquiry.**

35. **Section 2(7) of the Regulation of Investigatory Powers Act 2000 is particularly important and not enough attention has been paid to its significance.**

Role of the Information Commissioner

36. Given the fact that the aim of hacking is to obtain personal information, we thought it worth considering the various regulatory regimes dealing with the acquisition and use of information. Section 57 of the Regulation of Investigatory Powers Act creates the role of Interception of Communications Commissioner, but this role is limited to overseeing

those issuing warrants to the police and security services permitting interception, and those acting under warrant or assisting those acting under warrant. Generally, as its short title implies, the Act is concerned more with defining the powers of the state to intercept the communications of those present in the UK in the course of legal investigations than with private individuals or organisations attempting interception. This Commissioner has no duties in respect of private sector operators, and in particular has no remit or resources to advise individuals who believe they have been victims of unauthorised interception of their communications by the private sector. The Surveillance Commissioners also operate under the Regulation of Investigatory Powers Act and the Police Act 1997, but their job is to oversee the use by state officials of covert surveillance operations and covert human intelligence sources (otherwise known as undercover officers and informants), and not interception of communications.

37. We asked the Information Commissioner, Mr Christopher Graham, about his role in relation to telephone hacking. He replied that, although he and his office occasionally gave informal advice on the issues, he had no formal role under the Regulation of Investigatory Powers Act or the Misuse of Computers Act as he was not the prosecuting authority for either of these, and no one else had a regulatory role in respect of these Acts either:[14] he was appointed to oversee the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003. He added:

> Thus I have responsibility for taking action on the Data Protection Act s.55 offence that may arise from the unlawful 'blagging' of personal information from a data controller.[15] But the Information Commissioner does not have any regulatory competence in the area of interception of communication—which would cover hacking and tapping, for example, of mobile phone communications. This latter activity is dealt with entirely under the Regulation of Investigatory Powers Act. This means that the regulatory regime that covers the use, disclosure and interception of communications related data is fragmented.[16]
>
> The problem is that whilst the Data Protection Act, the Privacy and Electronic Communications (EC Directive) Regulations and the Regulation of Investigatory

14 Qq 155–161

15 'Blagging' is where an unauthorised person obtains personal information—addresses, telephone numbers, medical information, financial information, etc—from a source that legitimately hold the information by pretending to be either the individual whose information is held or someone else with a legitimate right to access the information.

16 Memorandum from the Information Commissioner, para 4

> Powers Act together form part of the framework of regulation that limits excessive surveillance and provides safeguards for individuals, it is only in relation to the Data Protection Act and Privacy and Electronic Communications (EC Directive) Regulations that there is an organisation charged with promoting compliance with the legislation and with providing authoritative advice to those who need it.[17]

38. One missing part of this fragmented regime has been provided by the entry into force on 25 May 2011 of new Privacy and Electronic Communications Regulations which provide that any data controller who becomes aware of a breach of data security must inform not only the Information Commissioner but also the affected customers.[18] Also, there was an attempt at a more joined-up approach to regulation in this area by bringing together the Information Commissioner with the three other regulators (the Surveillance and Interception of Communications Commissioners and the interim Closed Circuit Television Commissioner) to discuss any gaps in the regime.[19] We are concerned that this meeting appeared to be a rarity, and that there is not enough linkage between the different Commissioners.

39. **The lack of a regulatory authority under the Regulation of Investigatory Powers Act has a number of serious consequences. Although the Information Commissioner's office provides some advice, there is no formal mechanism for either those who know they are in danger of breaking the law or those whose communications may be or have been intercepted to obtain information and advice. Moreover, the only avenue if anyone is suspected of unauthorised interception is to prosecute a criminal offence, which, as the Information Commissioner noted, is a high hurdle in terms of standard of proof as well as penalty.[20] Especially given the apparent increase of hacking in areas such as child custody battles and matrimonial disputes,[21] and the consequential danger of either the police being swamped or the law becoming unenforceable, there is a strong argument for introducing a more flexible approach to the regime, with the intention of allowing victims easier recourse to redress. We therefore recommend the extension of**

17 *Ibid*, para 9.

18 Q 156

19 Qq 147–149

20 Memorandum from the Information Commissioner, para 8

21 Q 133 and *What Price Privacy Now?,* December 2006

the Information Commissioner's remit to cover the provision of advice and support in relation to chapter 1 of the Regulation of Investigatory Powers Act.

40. **We also strongly recommend that the Government reviews how the Act must be amended to allow for a greater variety of penalties for offences of unlawful interception, including the option of providing for civil redress, whilst retaining the current penalty as a deterrent for serious breaches.**

41. **We note that most of our witnesses claimed to be unaware at the time of the Information Commissioner's two 2006 reports, *What price privacy*? and *What price privacy now?*. We are disappointed that they did not attract more attention among the police, the media and in government, and hope that future such reports will be better attended to.**

42. **We are concerned about the number of Commissioners, each responsible for different aspects of privacy. We recommend that the government consider seriously appointing one overall Commissioner, with specialists leading on each separate area.**

43. In relation to blagging, there were limits on the Information Commissioner's powers:

> the Data Protection Act, insofar as it applies to this sort of thing, has a very broad exemption within it for what is called the special purposes, for literature, journalism and the arts. My investigatory powers can be very easily stymied by somebody telling me that what they are doing is for journalism, literature and the arts. All my powers of requiring information—information notices, investigation and the more dramatic stuff, kicking the door down—I can't do if there is an exemption for the special purposes. So my role in this area is, frankly, pretty limited.[22]

44. We questioned the Information Commissioner, Mr Christopher Graham, about the practical limits this placed on his investigations. He explained that, whereas in other situations any application by him to a court with reference to an information notice would be straightforward, it might not be worth spending the time and financial resources to challenge the recipient of the notice in court if he/she was or might be a journalist and the investigation that the person was carrying out might be in the public interest: "I am not

22 Q 133

sure I could make an information notice stick under these circumstances."[23] The Information Commissioner therefore considered that the legislation as currently drafted in practice seriously limited his ability to challenge the illegal obtaining of personal information by those who could legitimately claim to be journalists.

45. Furthermore, even where a case could be brought under section 55 of the Data Protection Act, the Information Commissioner considered that the penalties now available were inadequate, and he noted that magistrates were unwilling to impose even the maximum penalties currently available to them.[24] The maximum penalty for blagging under section 55 of the Data Protection Act is a fine of up to £5,000 in the magistrates court, although the fine may be higher if the case is prosecuted in the Crown Court.[25] He contrasted the situation with RIPA and the Misuse of Computers Act, which provide for a custodial sentence of up to two years as penalty for a breach. He noted that the Ministry of Justice was aware of the unsatisfactory situation in respect of the penalties attached to 'blagging' and that that department was exploring the possibility of bringing this activity within the ambit of legislation on restitution of the profits of crime [26] and talking to the Sentencing Advisory Council about recommending tougher penalties in its guidelines to magistrates.[27]

23 Qq 139–144

24 Qq 150–152

25 Section 60 of the Data Protection Act

26 The Information Commissioner estimated that the profits from the unlawful sale of personal information in the UK would amount to some millions of pounds per year: in one case alone, those selling the information were being paid £70,000 a week for the information: Qq 152–154

27 Q 151

3 The police response

Police response to hacking allegations

46. It would clearly be inappropriate for us to seek to interfere with the continuing police investigation into the News International hacking affair and the recently announced associated public inquiries, but it is necessary to undertake some examination of how the police responded to the allegations at various times.

The 2005–06 investigation and 2006-07 investigation

47. The hacking investigation began in December 2005 when the Head of Royalty Protection at the Metropolitan Police, Mr Dai Davies, told Mr Peter Clarke, then head of the Anti-Terrorist Branch, that members of the Royal Household were concerned that their voicemails were being accessed. Due to the potential security implications of, for example, the movements of members of the royal family becoming known, Mr Clarke said that the Anti-Terrorist Branch would investigate.[28] However, we note that the merger of the anti-terrorist and royal protection function of the Metropolitan Police is an alternative explanation for this decision. We were surprised that the previous Metropolitan Police Commissioner, Lord Blair of Broughton, said he had knowledge of these events.

48. As Deputy Assistant Commissioner at the time, Mr Clarke was responsible for setting the parameters of the inquiry. He described how he did so as follows:

> The parameters of the investigation, which I set with my colleagues, were very clear. They were to investigate the unauthorised interception of voicemails in the Royal Household, to prosecute those responsible if possible and to take all necessary steps to prevent this type of abuse of the telephone system in the future. The investigation would also attempt to find who else, other than Goodman and Mulcaire, was responsible for the interceptions. The reason I decided the parameters should be so tightly drawn was that a much wider investigation would inevitably take much longer to complete. This would carry, to my mind, two unacceptable risks. First, the investigation would be compromised and evidence lost and, second, that the much wider range of people, who we were learning were becoming victims of this activity,

28 Q 438

> would continue to be victimised while the investigation took its course. This would probably go on for many months and to my mind this would be unacceptable.[29]

As previously laid out, we were told that the investigation was further limited by the understanding that the correct approach was to attempt a prosecution under section 1 of the Regulation of Investigatory Powers Act, assuming a narrow interpretation of the offence, meaning that the police would have to find evidence that the voicemail had not been accessed by the intended recipient before it was accessed by the hacker.[30]

49. When Messrs Mulcaire and Goodman were arrested, the investigatory team, led by Mr Peter Clarke under the oversight of Mr Andy Hayman, requested a large amount of material from News International, including details of who Mr Mulcaire reported to, whether he had worked for other editors or journalists at the *News of the World*, records of work provided by him and details of the telephone systems in the *News of the World* offices. The police received a letter from the newspaper's solicitors saying that News International wished to assist, including with identifying any fellow conspirators, but the amount of relevant documentation was limited. In fact, very little material was produced. The police told us that they were unable to pursue the inquiry further with News International because of their refusal to co-operate.[31]

50. We pressed Mr Clarke on this issue, asking what prevented him from taking the matter further with News International despite the fact that he was, as he told us, "not only suspicious, I was as certain as I could be that they had something to hide."[32] Mr Clarke told us that what prevented him was the law: the police were advised by lawyers that, whilst News International through its lawyers was giving the impression of full co-operation, the police would not be able to obtain a 'Schedule 1 production order' to require disclosures of information as that might seem to amount to a 'fishing expedition'.[33] Mr Clarke said:

---

29 Q454 See also Qq 467-468

30 Ibid.

31 Q 457

32 Q 482

33 Qq 483–486 and Qq 332–334, 375. The law referred to is the Police and Criminal Evidence Act 1984, which provides a special regime for certain types of material which the police may wish to seize as evidence. Including material subject to legal privilege and journalistic material (sections 9, 11 and 13 of the Act). Under this regime, the police may obtain material acquired or created for the purposes of journalism only by means of a 'Schedule 1 application'. Schedule 1 provides that judges may make orders permitting the police to remove or have access to material connected with a crime provided that a number of conditions are all met to the judge's satisfaction. These include the condition that "other methods of obtaining the material have been tried without success.

> I think it has been explained many times before this Committee that there was correspondence entered into between us and News International. The letters that were sent from the Metropolitan Police were put together in consultation with the Crown Prosecution Service. The replies came back through the lawyers acting on behalf of News International and I know that the people, both from the CPS and from the Met, at the time who were looking at this were very frustrated at finding themselves in what they regarded as a legal impasse.[34]

51. **We deplore the response of News International to the original investigation into hacking. It is almost impossible to escape the conclusion voiced by Mr Clarke that they were deliberately trying to thwart a criminal investigation. We are astounded at the length of time it has taken for News International to cooperate with the police but we are appalled that this is advanced as a reason for failing to mount a robust investigation. The failure of lawbreakers to cooperate with the police is a common state of affairs. Indeed, it might be argued that a failure to cooperate might offer good reason to intensify the investigations rather than being a reason for abandoning them. None of the evidence given to us suggests that these problems were escalated for consideration by the Commissioner of the Metropolitan Police or by Ministers. The difficulties were offered to us as justifying a failure to investigate further and we saw nothing that suggested there was a real will to tackle and overcome those obstacles.**

52. In this context, we draw attention to the fact that, when we asked her on 5 July 2011 to comment on the allegations that the phones of the Dowler family had been hacked into, Ms Rebekah Brooks said in a letter of reply:

> I want to be absolutely clear that as editor of *News of the World* I had no knowledge whatsoever of phone hacking in the case of Milly Dowler and her family, or in any other cases during my tenure.
>
> I also want to reassure you that the practice of phone hacking is not continuing at the *News of the World*. Also, for the avoidance of doubt, I should add that we have no reason to believe that any phone hacking occurred at any of our other titles.[35]

In an earlier letter, responding to our request for clarification of the evidence on payment of police officers that she gave to the Culture, Media and Sport Committee in 2003, she said:

34 Q 484

35 Letter of 8 July 2011

> My intention was simply to comment generally on the widely-held belief that payments had been made in the past to police officers.
>
> If, in doing so, I gave the impression that I had knowledge of any specific cases, I can assure you that this was not my intention.[36]

Even this is not easy to reconcile with the record. **We note that neither of these carefully-crafted responses is a categorical denial: Ms Brooks's denial of knowledge of hacking is limited to her time as editor of News of the World; and on payments to police, she did not say that she had no knowledge of specific payments but that she had not intended to give the impression that she had knowledge of specific cases.**

53. The refusal by News International to co-operate with the police inquiry in 2005–06 meant that the only significant evidence available to the police lay within the 11,000 pages of documents that had been seized from Mr Mulcaire at the time of his arrest. Mr Clarke and his colleagues decided that the time and resource required for an exhaustive analysis of these papers could not be justified, but instead a team of officers was detailed to go through that material with a range of objectives; firstly, to look for evidence relevant to the offences that had been charged; secondly, to make sure that the police's obligations in terms of disclosure under the Criminal Procedure and Investigations Act were fulfilled; and thirdly, to look for potential victims where there were national security implications.[37] When we asked whether every document had been read at that time, Mr Clarke said that he could not say for sure whether it had: the team was instructed to look through the papers with particular objectives in mind, not to do an exhaustive analysis of every name, phone number and so on.[38] However, Mr Clarke did say that the team did not carry out its task on the narrow business of looking only for links between Mr Mulcaire and Mr Goodman: in the course of trawling through the papers, they identified 28 possible victims.[39]

54. We asked Mr Clarke why—given he was certain that the rot went wider—he had not followed the evidence by initiating a broader inquiry:

> ***James Clappison:*** In the normal course of policing, if an offence is discovered and it is discovered that there has been further offending associated with that offence, the police normally investigate the further offending, don't they? If, for example, you

36 Letter of 11 April 2011

37 Q 473

38 Q 477

39 Qq 518-520

> stop somebody for driving while disqualified and you find they have been committing burglaries, you would investigate the burglaries as well, wouldn't you?

He replied that the correct comparison was not with a crime such as burglary but with a complex fraud case where one would focus the investigation at an early stage, decide what the potential offences might be and then concentrate on trying to prove those offences.[40]

55. **The consequences of the decision to focus within the Mulcaire papers on the areas vital to the prosecution of Mulcaire and Goodman were extremely significant. A huge amount of material that could have identified other perpetrators and victims was in effect set to one side. Mr Clarke explained to us the reasons for taking this approach, starting with the context at the time.** He reminded us of the increase in the terrorist threat since 2002, and the London bombings and attempted bombings in the summer of 2005. He said that by early 2006 the police were investigating the plot to blow up trans-Atlantic airliners in midflight and those responsible were arrested on 9 August 2006, the day after Messrs Goodman and Mulcaire. **By the middle of 2006 the Anti-Terrorist Branch had more than 70 live operations relating to terrorist plots but some of these were not being investigated because there were not enough officers to do so. In this context, he had to decide on priorities, and the priority of protecting life by preventing terrorist attacks was higher than that of dealing with a criminal course of conduct that involved gross breaches of privacy but no apparent threat of physical harm to the public.**[41] **Nevertheless we cannot overlook the fact that the decision taken not to properly investigate led to serious wrongdoing which the Commissioner himself now accepts was disreputable.**

56. The second reason why the police decided not to do a full analysis of all the material was that they considered the original objectives of the investigation could be achieved through a number of other measures: the high-profile prosecution and imprisonment of a senior journalist from a national newspaper; collaboration with the mobile phone industry to prevent such invasions of privacy in the future;[42] and briefings to Government,

40 Q 465

41 Qq 459 and Q 512

42 We discuss this in greater detail below

including the Home Office and Cabinet Office, to alert them to this activity and to ensure that national security concerns could be addressed.[43]

57. We asked how many officers had been assigned to the investigation. We were told that the number varied but at the start of the investigation, because of the tight focus and the desire to limit the numbers with access to potentially sensitive information, the average was ten to twelve officers, and these formed the core during the investigation, with occasional support from analysts, intelligence officers and document readers. When it came to arrests and searches, officers were borrowed from elsewhere and maybe as many as 60 were involved.[44] This compares with an average of 45 officers who have been involved throughout in trawling through the Mulcaire papers and dealing with disclosure requests for the current investigation.

58. We also asked, given that counter-terrorism had to be his officers' priority, whether anyone had ever considered transferring responsibility for the non-terrorism related aspects of the case to other parts of the Metropolitan Police Service, such as the Specialist Crime Directorate:

> ***Alun Michael:*** Was any consideration given to stripping out the non-terrorism-related aspects of your command and putting these sorts of responsibilities, which could be seen as a distraction in those terms, to other parts of the Met, the Specialist Crime Directorate or whatever?
>
> ***Mr Clarke:*** I suppose you could say that this type of investigation was never core business for the Anti-Terrorist Branch. It came to us because of the national security issues at the beginning.
>
> ***Mr Clarke:*** Having got to that point, forgive me, is the point then that could I have tried to pass the investigation to somebody else? I think the realistic point—and I certainly thought about this at the time and it is reflected in the decision logs from the time—is that for the previous two years I had already been stripping out other parts of the Metropolitan Police to support the Anti-Terrorist Branch in a whole series of anti-terrorist operations. A lot of other serious crime had gone uninvestigated to the extent it should have done because of the demands I was placing on them. I took the view that it would be completely unrealistic, given that we were heading towards a prosecution of Goodman and Mulcaire, to then go to another department and say, "We've got a prosecution running. We have a huge

43 Q 458

44 Qq 513-515

amount of material here that needs analysing. We don't know, given the uncertainties of the legal advice, whether there will be further offences coming from this or not. Would you like to devote 50, 60, 70 officers for a protracted period to do this?" I took the judgment that that would be an unreasonable request and so I didn't make it.

Alun Michael: In your answer, you have indicated that other aspects were stripped out of the command in order to give you the maximum resource for dealing with terrorism. With the obvious benefit of hindsight, might it not have been better to shift this activity as well?

Mr Clarke: I don't honestly see where I could have shifted it to. It would have been more a case of trying to invite people, I think, to lend me more officers and, to be frank, I think I had tried their patience quite sufficiently over the past years. I don't mean it to sound trite but it would have been a very difficult request to have made to colleagues.

Alun Michael: But it wasn't pushed up the tree as a responsibility?

Mr Clarke: To be honest, there wasn't much of a tree to push up above me. I know this is something I discussed not only with my own colleagues in the Anti-Terrorist Branch but of course with Andy Hayman as well.[45]

59. Mr Clarke also addressed the question of whether his team could have returned to the unassessed material in the months after Messrs Goodman and Mulcaire's arrests. He said, "The answer quite simply is no. By December we were embroiled in the Litvinenko murder in London, and a few months later the attacks in Haymarket and Glasgow. Meanwhile, we had to service all the court cases that had been coming through the process for some years that in 2007 led to the conviction of dozens of people for terrorist-related crimes." He added that it would not have been feasible to ask other departments to undertake the task using their own scarce resources in a case where there had already been convictions and there was no certainty of obtaining convictions for serious offences, given the untested nature of the legislation.[46]

60. We asked whether Mr Clarke personally had been aware of the serious concerns about media breaches of privacy raised in two roughly contemporary reports from the Information Commissioner, *What price privacy?,* and its follow-up six months later, *What price privacy now?,* Mr Clarke said he had not been aware of them, probably because his

45 Qq 521–523

46 Q 459

focus was on terrorist issues, and if anyone else in the Metropolitan police had known of them they had not linked these reports with the Mulcaire investigation.[47]

61. **When challenged on whether he stood by his decision to limit the investigation in 2006, Mr Clarke said that, despite all that had been revealed since, he believed the decision to have been correct, given the limited resources at his disposal and the absolute priority of dealing with threats to public safety. We note this position. However, its consequences have been serious and we are not convinced that the former Commissioner's decision to merge anti-terrorist and royal protection functions on the basis that both involved firearms, or the decision to pursue this investigation within the command, were justified. It is also revealing about the nature of management within the Metropolitan Police Service that this issue does not appear to have been escalated to the Commissioner or Deputy Commissioner, or even the Assistant Commissioner, as an issue about which they ought to be aware and to which a solution needed to be found.**

62. Mr Clarke went further and said he considered that, in its own terms, the operation had been a success: the prosecutions had succeeded and the mobile phone industry had taken action to ensure that their customers were less vulnerable to the type of interception practised by Mr Mulcaire than before—so much so that "because of our work with the mobile phone companies in getting the protective security arrangements around voicemails changed, voicemail hacking no longer continues."[48] As we discuss in the next chapter, **whilst it is true that mobile phone companies have now acted to provide much greater security for their customers' communications, and whilst the 2005–07 inquiry succeeded on its own terms, we cannot say that inquiry was a success given the extent of the intrusion now becoming apparent and the fact that even now not all the victims of interception have been identified let alone contacted. Nor are we convinced that no hacking takes places or that it cannot take place. We do not have the technical**

47 Qq 504–505

48 Q 467

competence to make such a judgement, and nor did we receive detailed evidence on that point.

63. Mr Clarke's main regrets involved the consequences for victims of the decisions he had taken. One of the reasons why he thought a full trawl through the Mulcaire papers was not vital, was that he was putting in place a strategy for dealing with victims. As far as the people who had been identified by his officers were concerned, the strategy involved police officers informing certain categories of potential victim and the mobile phone companies identifying and informing others to see if they wanted to contact the police. As Mr Clarke acknowledged, he had since learned that this strategy did not work as intended. He also considered it "utterly regrettable" that the decision not to conduct a detailed analysis of all the material available had led to the failure to identify that victims of some of the most serious crimes were also among the victims of hacking—a category of people not previously considered to be potential targets.[49]

64. We also questioned Mr Andy Hayman, who at the time had been Assistant Commissioner in charge of the Specialist Operations Group and Mr Peter Clarke's immediate superior officer. We wanted to explore Mr Hayman's role in the 2006 investigation, not least in the light of the fact that he was known to have had a number of meals with senior News International figures at the time and had subsequently, shortly after his resignation from the Metropolitan Police in 2008, started to write a regular column for *The Times*.[50]

65. Mr Hayman denied that anything improper or unprofessional had occurred, either in relation to his informal contacts with News International at the time or in relation to his subsequent employment by them. On the dinners, he said that he had not revealed anything about the hacking investigation, not least because Mr Clarke was, for security reasons, minimising the number of people kept informed about the investigation so Mr Hayman did not know the details himself. Mr Hayman said whilst he was accountable for what was done and had oversight of the investigation, the day-to-day responsibility was Mr

49 Qq 458-459

50 For *the Times* column, see Qq 528–532

Clarke's and he was not even aware that Mr Clarke considered News International was being very obstructive in relation to the investigation.[51] He stated that he had had no involvement in the decision to set narrow parameters for the inquiry, nor in the decision not to comb through the 11,000 pages of the Mulcaire documents. He said that he could not remember the detail of his daily briefings from Mr Clarke, but said that he had been aware of the CPS advice and had endorsed all Mr Clarke's decisions about strategy and approach.[52]

66. **Mr Hayman claims to have had little knowledge of the detail of the 2006 operation, and to have taken no part in scoping it or reviewing it; his role seems to have been merely to rubber-stamp what more junior officers did. Whilst we have no reason to question the ability and diligence of the officers on the investigation team, we do wonder what 'oversight', 'responsibility' and 'accountability'—all of which words were used by Mr Hayman to describe his role—mean in this context.**

67. **Leaving aside the fact that his approach to our evidence session failed to demonstrate any sense of the public outrage at the role of the police in this scandal, we were very concerned about Mr Hayman's apparently lackadaisical attitude towards contacts with those under investigation. Even if all his social contacts with News International personnel were entirely above board, no information was exchanged and no obligations considered to have been incurred, it seems to us extraordinary that he did not realise what the public perception of such contacts would be—or, if he did realise, he did not care that confidence in the impartiality of the police could be seriously undermined.**

68. Mr Hayman was very vague about the number of dinners and other events that occurred during the time of the 2005–07 investigation, but he stated that he had always been accompanied by the Director of Communications of the Metropolitan Police.[53] We have subsequently received evidence from the Director of Communications that, to the

51 Qq 534–536 and 544

52 Qq 562–570

53 Qq 534–535

best of his recollection, he accompanied Mr Hayman only once to a social event with News International:

> I first became aware of the investigation into phone hacking upon my return from a period of leave in August 2006.
>
> To the best of my knowledge and recollection, the only dinner that I attended with Mr Hayman and News International staff was on 25 April 2006, some three months previously. The dinner was entered in the Specialist Operations Directorate Hospitality Register.
>
> Therefore, I did not discuss with, or give advice to, Mr Hayman on any question relating to attending this dinner whilst the investigation was in progress. Furthermore, I did not have any conversation with Mr Hayman about phone hacking more generally at that time. [54]

We do not expressly accuse Mr Hayman of lying to us in his evidence, but it is difficult to escape the suspicion that he deliberately prevaricated in order to mislead us. This is very serious.

69. **Mr Hayman's conduct during the investigation and during our evidence session was both unprofessional and inappropriate. The fact that even in hindsight Mr Hayman did not acknowledge this points to, at the very least, an attitude of complacency. We are very concerned that such an individual was placed in charge of anti-terrorism policing in the first place. We deplore the fact that Mr Hayman took a job with News International within two months of his resignation and less than two years after he was—purportedly—responsible for an investigation into employees of that company. It has been suggested that police officers should not be able to take employment with a company that they have been investigating, at least for a period of time. We recommend that Lord Justice Leveson explore this in his inquiry.**

Assistant Commissioner Yates's role

70. Following the conviction of Messrs Mulcaire and Goodman, the papers seized from Mr Mulcaire were stored in evidence bags and the police seem to have expected no further action would need to be taken. The case was considered closed.[55] However, *The Guardian* newspaper continued to investigate whether other journalists and editorial staff from the

54 Letter from Dick Fedorcio, 8 July 2011

55 Letter from Yates to Chair, 8 July 2011

News of the World had made use of Mr Mulcaire's services to obtain information illegally. On 8 July 2009, *The Guardian* published a story that Mr Gordon Taylor, head of the Professional Footballers Association, had been paid a substantial sum by News International to stop him speaking about the alleged hacking of his mobile phone. The obvious inference was that it was unlikely the royal correspondent of the *News of the World* would have been interested in Mr Taylor's messages so other journalists must also have been involved in hacking. As stated earlier, this and other stories led the Commissioner of the Metropolitan Police on 9 July 2009 to put Assistant Commissioner John Yates in charge of examining the allegations. This process has been frequently referred to as a 'review' of the earlier investigation, but Mr Yates told us: "From the beginning of my involvement in this matter in 2009, I have never conducted a 'review' of the original investigation and nor have I ever been asked to do so." He told us that 'review' has a specific meaning for the police, "a review, in police parlance, involves considerable resources and can either be thematic in approach—such as a forensic review in an unsolved murder investigation—or involves a review of all relevant material." [56] Mr Yates told us that the Commissioner had asked him to "establish the facts around the case and to consider whether there was anything new arising in the *Guardian* article. This was specifically not a review. [*Mr Yates's emphasis*]"[57]

71. The form of Mr Yates's consideration of the hacking allegations appears to have been that he received detailed briefings from the Senior Investigative Officer for the 2005–07 investigation, including considering the CPS's contemporaneous advice (he did not take fresh legal advice), and after discussing it with some of the officers involved in the investigation he came to the conclusion that the *Guardian* articles gave no new information unknown to the police in 2005–07 that would justify either re-opening or reviewing the investigation. The whole process took about eight hours.[58] At that time, Mr Yates also took the decision that the material seized from Mr Mulcaire should be listed on a

56 Letter to Committee of 8 July 2011

57 Ibid.

58 Ibid. And Qq 327, 335–336, 364–369, 386–388, 390, 394–401, 406–408

database so that it would in the future be easier to see whether new evidence could be linked to any existing evidence.[59]

72. At the same time, the Director of Public Prosecutions had ordered an urgent examination of the material supplied to the CPS. Such a review by the CPS "is always undertaken in relation to relevance in respect of the indictment", although Mr Yates stresses that the CPS saw all material available to the Met. It appears that the CPS review only reconsidered whether all the material relevant to the original indictment of Messrs Mulcaire and Goodman in relation to the six charges in 2007 had been dealt with thoroughly. However, in a written memorandum dated 14 July 2009, Counsel confirmed that the CPS had asked about the possibility of the then editor of the *News of the World* or other journalists being involved in the Goodman-Mulcaire offences, but had never seen any evidence of such involvement. We were told by the current Director of Public Prosecutions that at this time, in July 2009, the police and CPS discussed the mention in the papers of the name 'Neville'—which was taken possibly to refer to Mr Neville Thurlbeck, ex-chief reporter of the *News of the World*. The DPP, however, concluded that the name 'Neville' was not enough to warrant re-opening the investigation, and Mr Thurlbeck was not interviewed.[60] At the end of the CPS review, the Director of Public Prosecutions said that "it would not be appropriate to re-open the cases against Goodman and Mulcaire or to re-visit the decisions taken in the course of investigating and prosecuting them."[61]

73. **In short, the exercises conducted by the police and the CPS in July 2009 appear to have been limited to the consideration of whether or not, in the light of recent reports in the media, the 2005–07 investigation had been carried out thoroughly and correctly. Critically, because the 2005–07 investigation had focused only on the joint roles of Messrs Mulcaire and Goodman, there was no progress in 2009 to consideration of the**

59 Q 372

60 Qq 399–401

61 Yates letter of 8 July, Press release from the CPS dated 16 july 2009 and Qq 337–338

relationships that Mr Mulcaire might have had with other journalists, even though the Gordon Taylor story implied that such relationships had existed.

74. On 1 September 2010, just before AC Yates first gave oral evidence to us, the New York Times reported comments comments by the late former News International journalist, Mr Sean Hoare, about the involvement of former colleagues in hacking. This led Mr Yates to undertake a scoping study—in other words, to appoint a Senior Investigating Officer to ascertain whether the new information published in the *New York Times* was sufficient to justify (re)opening an investigation.

75. On 7 September, we asked Mr Yates about his approach to the new allegations:

> **Q22 Alun Michael:** Can I just clear up one simple point? You referred to speaking to and interviewing a number of people, and a letter that is going today to the *New York Times* and so on. Would I be right in interpreting what you have said as meaning there is now a live investigation taking place?
>
> ***Mr Yates:*** I think it's a semantic point. What constitutes a reopened investigation? If we are going to speak to somebody, some people will say that is a reopened investigation. I would say we are considering new material and then we will work with the CPS to see whether that constitutes potential lines of inquiry that can be followed up and would be likely to produce evidence and be a proper use of our resources.
>
> **Q23 Alun Michael:** I suppose I would put it another way. Is it just a question of having some discussions or are you actively seeking to be able to say to the public that the issues have been fully investigated?
>
> ***Mr Yates:*** Mr Hoare has made some very serious allegations both in print and on the radio, and clearly we need to go and speak to him to see what he has to say about that in the broader context.[62]

Rather than being 'a semantic point', we consider the evidence given to us by Mr Yates to be totally unclear. There was considerable ambiguity about the status and depth of the police enquiries, and it was not clear whether the purpose was to respond to potential criticism of the earlier inquiries or to genuinely pursue the evidence to a clear conclusion. This is one reason that we kept our own inquiry open in the hope of obtaining greater clarity in due course.

62 Yates evidence on *Specialist Operations*

76. Again, apparently because witnesses were unwilling to come forward, the CPS decided on 10 December 2010 that there was insufficient evidence to provide a realistic prospect of conviction against any of the people identified in the *New York Times*.[63]

77. However, the situation changed completely very early in January 2011. As a result of the continuing civil proceedings being brought by people who believed themselves to have been victims of hacking, disclosure requirements were imposed on the police by the courts and—arguably in response to these disclosures—News International decided to suspend Mr Ian Edmondson on 5 January and thereafter to provide new information to the police about the scope of complicity by other employees in the hacking by Mr Mulcaire. On 14 January 2011 the Director of Public Prosecutions announced that the CPS would conduct a "comprehensive assessment of all material in the possession of the Metropolitan Police Service relating to phone hacking, following developments in the civil courts", which would "involve an examination of all material considered as part of the original investigation into Clive Goodman and Glenn Mulcaire and any material that has subsequently come to light." [64]The assessment was to be carried out by the Principal Legal Advisor, Alison Levitt QC.

78. On 26 January 2011, the Metropolitan Police announced it was launching a new inquiry into alleged phone hacking as a result of receiving "significant new information from News International relating to allegations of phone hacking at the News of the World in 2005/06." The new investigation was to be led by DAC Sue Akers and carried out by the Specialist Crime Directorate which had, according to the press notice announcing the inquiry, been investigating a related phone hacking allegation since September 2010.[65] It was agreed with the CPS that Alison Levitt would continue her re-examination of the existing material.

79. We pressed Mr Yates repeatedly on why the scope of the exercises in 2009–10 had been so narrow, when he was aware of the earlier Operation Motorman which—though not

63 Quoted in letter from Yates to Committee of 8 july

64 CPS Press Notice of 14 january 2011, 'DPP announcement on phone hacking'

65 'New investigation regarding alleged phone hacking', Press Notice dated 26 January 2011

related to hacking—revealed journalists' widespread use of blagging and other illegal methods of obtaining information.[66] He replied:

> It is a very fair question, but you talked about command decision. What you have to do occasionally, you do take decisions, you base them on risk and you consider them fully about what are the other issues, and I have given you the levels of reassurance I had. There was simply no reason at that time. The ICO is a completely different matter, it judges on a different standard of evidence against different offences. It was a decision taken. Now, in the light of what we now know, it was not a very good decision, but it is solely—I will repeat it—it is solely as a result of the new information provided by News International who clearly misled us. They clearly misled us.
>
> **Nicola Blackwood:** Was there a feeling that you were going to do the minimum necessary in order to show that you had looked at the facts and that there was nothing new in this case because you have more important things to be getting on with?
>
> ***AC Yates:*** There is probably an element of that but if there had been any new evidence there, if I had seen any new evidence there, then of course—
>
> **Nicola Blackwood:** But you did not even take new legal advice, so you just looked at the documentation from before.
>
> ***AC Yates:*** I was supported later by the DPP and by counsel.[67]

80. **We understand that, when Sir Paul announced in July 2009 that he was asking Mr Yates to look into any new information, this was an unprepared remark made as he was going into the ACPO conference rather than a carefully prepared statement.[68] Unfortunately it left the public—and indeed Parliament—with the impression that a more detailed examination was to be held than was in fact the case.**

81. **We assume that Sir Paul left Mr Yates with a large amount of discretion as to how he should consider the evidence. Mr Yates has subsequently expressed his view that his reconsideration in 2009 of the material available from the earlier investigation was very poor.[69] We agree. Although what Mr Yates was tasked to do was not a review in the proper police use of the term, the public was allowed to form the impression that the**

66 Qq 376–378, 381–385

67 Qq 382–384

68 Letter of Sir Paul to Committee dated 13 July 2011

69 Q 325

material seized from Mr Mulcaire in 2006 was being re-examined to identify any other possible victims and perpetrators. Instead, the process was more in the nature of a check as to whether a narrowly-defined inquiry had been done properly and whether any new information was sufficient to lead to that inquiry being re-opened or a new one instigated. It is clear that the officers consulted about the earlier investigation were not asked the right questions, otherwise we assume it would have been obvious that there was the potential to identify far more possible perpetrators in the material seized from Mr Mulcaire. Whether or not this would have enabled the police to put more pressure on News International to release information, by making it clear that police inquiries were not merely a 'fishing expedition' but targeted at certain people, is an issue that may be addressed by the forthcoming public inquiry.

82. **Mr Yates has apologised to the victims of hacking who may have been let down by his not delving more deeply into the material already held by the police. We welcomed that and agree that his decision not to conduct an effective assessment of the evidence in police possession was a serious misjudgement.**

83. As we were finishing our inquiry, the news broke that Sir Paul Stephenson and Assistant Commission Yates has resigned, and that the Metropolitan Police Authority has referred to the IPCC complaints about their conduct and the conduct of Mr Peter Clarke, Mr Andy Hayman and Mr Dick Fedorcio. The Deputy Chair of the IPCC had made a statement that the IPCC would carry out an independent investigation of the matters referred.

84. We asked Sir Paul, Mr Yates and Mr Dick Fedorcio, Director of Public Affairs at the Metropolitan Police, about the allegations being circulated in the media, about the employment of Mr Neil Wallis, former deputy editor of the News of the World. Assistant Commissioner Yates admitted to us that he was a friend, though not a close friend of Mr Wallis. In September 2009 Mr Wallis, who had resigned from his employment from News International was employed on a 'retainer contract' to assist Mr Fedorcio during the illness of Mr Ferdorcio's deputy. The contract was on a rolling 6 month basis and was renewed twice. Just after the second renewal, on 7 September 2010. Stories in the New York Times

about hacking by News International journalists led Mr Ferdorcio and Mr Wallis to come to the conclusion that the relationship now might lead to embarrassment and to continue the contract was inappropriate.

85. We examined the process for appointing Mr Wallis. We were told that three quotes were invited: Mr Wallis' was by far the lowest. On the question of whether due diligence had been performed in relation to Mr Wallis, Mr Fedorcio said that he had consulted AC Yates. AC Yates said that he had asked Mr Wallis informally about whether anything in his past might be a source of embarrassment to him, the Met or Mr Wallis himself, Mr Wallis told him he need have no concerns. Mr Yates completely denied the suggestion that what he had done at all deserved the description of 'due diligence'; he argued he had sought informal assurances to satisfy himself, and this was completely separate from the objective process of assessment and awarding of contracts.

86. **We are appalled at what we have learnt about the letting of the media support contract to Mr Wallis. We are particularly shocked by the approach taken by Mr Fedorcio: he said he could not remember who had suggested seeking a quote from Mr Wallis; he appears to have carried out no due diligence in any generally recognised sense of that term; he failed to answer when asked whether he knew that AC Yates was a friend of Mr Wallis; he entirely inappropriately asked Mr Yates to sound out Mr Wallis although he knew that Mr Yates had recently looked at the hacking investigation of 2005-06; and he attempted to deflect all blame on to Mr Yates when he himself was responsible for letting the contract.**

The new investigation

87. As described by DAC Akers, the catalyst for the new investigation was the civil actions against News International brought by a number of people who suspected that they had been victims of hacking. These actions involved legal requests for a "vast amount" of disclosure from news International and, in the process of trawling through their e-mail and other records, News International found three key e-mails implicating an employee other

than Mr Goodman in hacking. These were passed to the police in January 2011 and led to the launch of the new inquiry.[70]

88. We asked DAC Sue Akers about progress in the new investigation. She said that in the six months since it started, there had been eight arrests. Her team of 45 officers were still compiling lists of all the material seized in 2006 as the database started under AC Yates's auspices had not worked properly. However, she assured us that the material would be examined thoroughly and, if it led to suspicions about journalists inside or outside the News International group, the investigation would follow that evidence.[71] As for relations with News International, she explained that these had been difficult at first when most of the contact was with News International's lawyers and it had taken two months to agree a protocol on journalistic privilege.[72] However, following a meeting between News International executives and the police to discuss their "very different interpretations of the expression 'full co-operation'", relations had improved markedly.[73]

89. In order to reassure the public and all those who feared that they might have been targets of hacking, she had adopted a different approach from her predecessors': instead of addressing only those who were definitely victims of crime, she had decided they should contact everyone whose name or phone number appeared in the Mulcaire papers and who could be identified from the information available. She said there were in the region of 3,870 full names of individuals in the evidence already held by the police, plus about 5,000 landline numbers and 4,000 mobile numbers. However, when we asked her how many of these people had been contacted so far, the figure she gave was 170. Many others—approximately 500—had contacted her team asking whether their details were recorded in Mr Mulcaire's papers; only 70 of these had been definitely identified as potential victims. She noted that her team also had the task of responding to disclosure requests in connection with the civil actions that were continuing; she indicated that this was very time-consuming and was significantly slowing down the investigation. It was therefore

70 Qq 605 and 627–632

71 Qq 606, 612, 635–638 and 640

72 The problem relating tosection 55 of the Data Protection Act discussed in paragraphs x-y above

73 Qq 622–623

impossible to predict when the investigation would be complete, though she drew attention to the fact that those arrested had been bailed to appear in October, which gave an indication of the minimum timescale.[74]

90. We asked DAC Akers about the fact that some of the material recently handed over to the police by News International revealed that newspapers had made payments to some police officers, and that the Commissioner of the Metropolitan Police had put her in charge of investigating this. DAC Akers said that, as a result of having become aware of these allegations on 20 June with more material being supplied on 22 June, she had met the Independent Police Complaints Commission ('IPCC')and it was agreed with them that she should continue to "scope" a possible investigation. On 7 July, the matter was formally referred to the IPCC by the Metropolitan Police. In technical terms, it was a 'supervised investigation' under the personal supervision of the Deputy Chair of the IPCC: this meant that, whilst DAC Akers retained direction and control of the investigation, the Deputy Chair of the IPCC was kept fully appraised of what was happening.[75]

91. **From the point of view of victim support and of reassurance to the public, DAC Akers's decision to contact all those who can be identified as of interest to Mr Mulcaire is the correct one. However, this is not the same as saying all these people were victims of hacking, let alone that they could be proved to be victims. Only 18 months' worth of phone data from the relevant period still exist: unless Mr Mulcaire provides a list, no one will ever know whose phone may have been hacked into outside that period. Within the 18-months data held, about 400 unique voicemail numbers were rung by Messrs Mulcaire or Goodman or from News of the World hub phones, and these are the voicemails likely to have been hacked into. The total number of people who may eventually be identified as victims of Mr Mulcaire's hacking is therefore much lower than the number of names in his papers.**

92. **DAC Akers gave us a guarantee that this further investigation would be carried out thoroughly. We were impressed by her determination to undertake a full and searching**

74 Qq 608, 637, 611, 639 and 616–617

75 Qq 613–614

investigation. The Specialist Crime Directorate is clearly the correct place for an investigation of this sort, though we note that officers have had to be 'borrowed' from across the Metropolitan Police Service to meet the needs of this particularly labour-intensive inquiry.

93. **We note with some alarm the fact that only 170 people have as yet been informed that they may have been victims of hacking. If one adds together those identified by name, the number of landlines and the number of mobile phone numbers identified (and we accept that there may be some overlap in these), that means up to 12,800 people may have been affected all of whom will have to be notified. We accept that there are a number of reasons why progress may have been slow so far, but at this rate it would be at least a decade before everyone was informed. This timeframe is clearly absurd, but it seems to us to underline the need for more resources to be made available to DAC Akers. We understand that in the current situation of significant budget and staff reductions, this is very difficult. However, we consider that the Government should consider making extra funds available specifically for this investigation, not least because any delay in completing it will seriously delay the start of the public inquiry announced by the Prime Minister.**

94. **We are seriously concerned about the allegations of payments being made to the police by the media, whether in cash, kind or the promise of future jobs. It is imperative that these are investigated as swiftly and thoroughly as possible, not only because this is the way that possible corruption should always be treated but also because of the suspicion that such payments may have had an impact on the way the Metropolitan police may have approached the whole issue of hacking. The sooner it is established whether or not undue influence was brought to bear upon police investigations between December 2005 and January 2011, the better.**

95. **We are concerned about the level of social interaction which took place between senior Metropolitan Police Officers and executives at News International while investigations were or should have been being undertaken into the allegations of phone hacking carried out on behalf of the News of the world. Whilst we fully accept the**

necessity of interaction between officers and reporters, regardless of any ongoing police investigations senior officers ought to be mindful of how their behaviour will appear if placed under scrutiny. Recent events have damaged the reputation of the Metropolitan Police and led to the resignation of two senior police officers at a time when the security of London is paramount.

4 The role of the mobile phone companies

96. To date in the various parliamentary, police and media inquiries into phone hacking, there has been little focus on the role of the mobile phone companies in advising customers on security, protecting the data of their customers, and in notifying customers of any suspected breaches of security or data protection.

97. We were aware that the few possible victims of hacking by Mr Mulcaire already firmly identified by April this year had been customers of three leading mobile phone companies: O2, Vodafone, and the joint venture between Orange UK and T-Mobile UK which is called 'everything everywhere' (because these names are more familiar, we use the form 'Orange UK/T-Mobile UK' for the joint venture in this report). We also received some information from 'Three' describing its security procedures relating to voicemail, but since—as of 8 June 2011—it had had no indication that any of its customers had been victims of hacking, we did not pursue more detailed inquiries with that company.

How the hacking was done

98. Mobile phone companies have for some years offered the service to customers of being able to access their voicemails either from their own handsets or, using a PIN number, from another phone. In order to carry out his operations, Mr Mulcaire had to obtain the mobile phone numbers and the voicemail pin numbers of his quarry. In 2005–06, there were considerable variations between mobile phone companies in the ease of accessing voicemails. Handsets often came with a default PIN number for accessing voicemail and, it has been suggested, many of the victims may not have changed the standard default settings on their phones. Hackers knew that there were a limited number of default numbers and could at least try those first. O2 told us that before 2006 customers could use the default number for access and were not required to register a personal voicemail PIN; Vodafone's system seems to have been similar as it said that prior to 2006 customers were "able to" (not 'required' to) change their voicemail PIN to a number of their choosing; default PINs were removed on T-Mobile in 2002 and had never existed on Orange, so from

2002 onwards customers of both companies were unable to access voicemail remotely without a personal PIN. [76]

99. In oral evidence in September 2010, AC Yates said: "When the investigation started in 2006, it was a catalyst for the service providers to provide proper direct and more prescriptive security advice rather than what most people did in the past, which is leave their PIN number as the factory setting."[77]

100. In some circumstances, even when a customer had set a personal PIN number but forgotten this, it was possible to ask the phone company to reset the PIN to default or a temporary PIN number, if the person requesting it passed security checks such as the provision of registered personal information.[78] Unfortunately, this sort of information is often easy for a hacker to guess or ascertain if the customer is well known.

101. However, given DAC Akers's evidence that about 400 unique voicemail numbers were rung from Mr Mulcaire's, Mr Goodman's or News of the World hub phones,[79] it is possible that Mr Mulcaire obtained some of the information he needed for hacking from the mobile companies by either pretending to be someone with a legitimate right to the information or by bribing an employee for information. We therefore tried to discover whether phone company staff may have had access to personal PIN numbers, which they may have been either deceived or bribed into passing on.

102. O2 said that staff did not have access to customers personal voicemail PIN numbers even before 2006.[80] Vodafone UK told us that personal PINs were held on an encrypted platform which had always been inaccessible to its staff.[81] Orange UK/T-Mobile UK said that the voicemail PIN was not stored in any readable format within either T-Mobile or Orange UK "and therefore we do not consider it possible for anyone to obtain a customer's

76 Letters from Vodafone and O2 of 6 July and Orange of 14 July

77 Q 26, oral evidence on Specialist Operations of 7 September 2010

78 O2 letter of 6 July and May letter from OrangeUK/T-Mobile UK

79 Letter of 6 July 2011

80 Letter of 6 July 2011

81 Letter of 6 July 2011

unique PIN via our systems."[82] However, Orange UK/T-Mobile UK noted that Customer Service Advisers may change PIN numbers at the request of customers who have, for example, lost their phones. Whilst customers may subsequently change the number again through their own handset, unless and until they do so the Customer Service Adviser knows their PIN.[83]

103. Of the three mobile companies which we knew had had customers identified as possible hacking victims of Mr Mulcaire, only one directly answered our question: Did you carry out any investigation to discover how Mr Mulcaire had obtained access to customers' PIN numbers? Vodafone told us: "Yes. ... it appears that attempts may have been made by an individual/individuals to obtain certain customer voicemail box numbers and/or PIN resets from Vodafone personnel by falsely assuming the identity of someone with the requisite authority (such as the relevant customer)."

104. In his Adjournment Debate on Mobile Communications (Interception) on 10 March 2011, Mr Chris Bryant MP said: "There is clear evidence that in some cases rogue staff members [of mobile phone companies] sold information to investigators and reporters."[84] We attempted to discover whether that may have happened in this case. We asked: 'Were any members of your staff disciplined followed the release of PIN numbers; and, if so, how many?' Vodafone replied that, given it was not clear exactly how many and which of its customers had been affected by the Mulcaire case, and given the nature of the deception that may have been practised on its staff, it was not in a position to investigate the matter, let alone discipline anyone.[85] O2 said: "We found no evidence to suggest that any of our staff disclosed PIN numbers (which is consistent with our investigation that found that voicemails were accessed through use of the default PIN number). No employee, therefore, was disciplined."[86] Orange UK/T-Mobile UK said: "We have no evidence of any Orange UK or T-Mobile UK staff involvement related to this hacking incident therefore there was

82 May letter

83 Letter of 14 July 2011

84 HC Debate, col 1171

85 May letter

86 May letter

no requirement to take disciplinary action. Importantly, the systems we operate mean that individual staff members do not have access to a customer's PIN number. They would only ever know the PIN number when a temporary PIN is issued ... and this would only be done when the customer had successfully passed through our security process to verify their identity."

105. **We note that, despite these protections, each of the companies had identified about 40 customers whose voicemails appeared to have been accessed by Mr Mulcaire. We also note that all three companies have disciplined or dismissed employees for unauthorised disclosure of customer information in the last ten years,[87] though there is no indication that any of these employees was linked to this case.**

Measures taken since to deter hacking

106. In his evidence to us, Mr Bryant was asked what mobile phone companies should do to protect their customers' privacy better. He replied:

> I think they need stronger internal mechanisms to make sure that PIN numbers aren't available to be handed out by somebody when ringing into a mobile phone company. I think all the phone companies should adopt the same processes as well because people do often change from one company to another. I think it would be a good idea if they always notified somebody when there was any doubt about whether their phone was being accessed illegally, which is not the policy of all the mobile companies at the moment. Some of them do it and some of them don't, which is why, for instance, in my case I rang Orange and found out seven years after the occasion that my phone had been accessed back in 2003.[88]

107. Very soon after the police began their inquiry into Mr Mulcaire, and arguably as a result of that investigation, the mobile phone companies reviewed and changed the way in which they allowed customers to access their voicemails remotely (ie not from their own handsets). Whereas previously Vodafone's customers had been able to contact Customer Services to request that the PIN number be manually reset to a number of their choice, Vodafone tightened up the operation by providing that new PIN numbers could be issued only via SMS message direct to the customer's own handset. Vodafone also subsequently

87 Letters of 6 July and 14 July 2011

88 Q 27 (oral evidence of 27 March)

installed a new, more secure voicemail platform, with additional procedures in place to warn customers in the event of unsuccessful remote attempts at access.[89] O2 changed its voicemail service so that customers cannot access their voicemails remotely at all unless they have registered a personalised PIN number.[90]

108. When he was asked what more mobile phone companies should be doing to improve security, the Information Commissioner highlighted a lack of information for the public:

> I wish they were a bit noisier about advising their customers on how they can keep their information secure. It is a general point, I think. There are responsibilities on communication service providers and internet service providers, and there are also things that individual consumers and citizens can do, but you kind of have to be told about them to know what it is you can do. We recently did some survey work and found that a very high proportion of people had no idea whether their home wi-fi was passworded or not. That is a pretty basic step. I wonder how many of us are very, very careful to password protect our mobile phones, not just the voicemail mailbox but also the machine itself, the device itself. I would like the mobile phone operators to be much louder in their advice to customers saying, "Look, your Smartphone, your iPhone, it's a wonderful thing, you can do fantastic things on it but there's a downside. Be careful, make sure you've set appropriate permissions, make sure you've set appropriate passwords." That should not be in the small print of some agreement written in lawyer-speak that nobody can understand; it should up front, user-friendly advice.[91]

109. However, he considered that the situation was improving:

> I have found that the mobile phone companies are getting much better at this. I have been invited to give presentations to global privacy conferences by two of our leading mobile providers recently. They really are interested. The reason they are interested is, I think, they have got that we are now beyond the stage of kiddies in the sweet shop bowled over by the wonders of what we can see; we are a bit more questioning. .... There is a commercial reason for treating customers with respect.[92]

110. As mentioned above, the Information Commissioner also explained that, under the new Privacy and Electronic Communications Regulations which came into effect on 25 May 2011, from now on any data controller, including a mobile phone company, which becomes aware that data security has been breached must inform its customers of this.

89 May letter

90 May letter

91 Q 162 (oral evidence of 26 April)

92 Q 162

111. **We welcome the measures taken so far to increase the security of mobile communications. However, with hackers constantly developing new techniques and approaches, companies must remain alert. In particular, it is inevitable that companies will think it in their interest not to make using technology too difficult or fiddly for their customers, so do not give as much prominence to the need to make full use of all safety features as they should do. We would like to see security advice given as great prominence as information about new and special features in the information provided when customers purchase new mobile communication devices.**

Notifying the victims

112. Mr Peter Clarke told us that he had established a strategy for informing the potential victims of Mr Mulcaire's hacking, with the police contacting certain categories of potential victim and the mobile phone companies identifying and informing others to see if they wanted to contact the police. He had not been aware that this had not worked.

113. We were told that from an early stage the investigation team were in close contact with, and had co-operation from, all the main mobile phone service providers. This was supplemented by communication via the Mobile Industry Crime Action Forum and its Chair. However, whilst each of the companies was well aware of the investigation, only one of those from whom we took evidence (O2) actually took the step of contacting their customers at the time to inform them that their voicemail messages might have been intercepted. It is worth setting out their reasoning in full.

114. O2 said that, when they had checked with the police that this would not interfere with the investigation: "As soon as the above customers were identified, we contacted the vast majority by telephone to alert them that there may have been a breach of data. There were a small number of customers who were members of a concierge service that were contacted directly by that service rather than O2. There were also a small number of customers that the Police contacted directly for security reasons;" and "We informed the customers that they were potential targets for voicemail interception and changed their voicemail PIN

numbers. We also offered to put them in touch with the Metropolitan police, if they wished to discuss this matter with the investigation team."[93]

115. Vodafone's response to the investigation was less direct: "mindful of the need to avoid undermining the ongoing Police investigation and/or jeopardising any subsequent prosecutions, Vodafone sought to contact the above customers in August 2006 to remind them to be vigilant with their voicemail security."[94]

116. Orange UK and T-Mobile UK at first told us: "We have not had any cause to suspect that particular mailboxes have been unlawfully accessed, and accordingly we have not needed to notify the relevant customers."[95] They subsequently explained that they considered it inappropriate to take any action in respect of their customers: " as any direct contact with customers could jeopardise the ongoing Police investigation and prejudice any subsequent trial. This is our standard approach when assisting in police investigations."[96]

117. **Clearly, Mr Clarke's strategy for informing victims broke down completely and very early in the process. It seems impossible now to discover what went wrong in 2006. Some of the mobile companies blamed police inaction: both Vodafone and Orange UK/T-Mobile UK said that the police had not told them to contact their customers until November 2010. AC Yates accepted that some of the correspondence between the police and the companies had not been followed up properly.[97] However, the companies cannot escape criticism completely. Neither Vodafone nor Orange UK/T-Mobile UK showed the initiative of O2 in asking the police whether such contact would interfere with investigations (and O2 told us that they were given clearance to contact their customers only ten days or so after being informed of the existence of the investigation). Nor did either company check whether the investigation had been completed later. They handed over data to the police, Vodafone at least sent out**

93 May letter

94 May letter

95 Written ev of October 2010, para 14

96 May letter

97 Q 433

generalised reminders about security (Orange UK/T-Mobile UK may not even have done that), they tightened their procedures, but they made no effort to contact the customers affected.

118. **We find this failure of care to their customers astonishing, not least because all the companies told us that they had good working relationships with the police on the many occasions on which the police have to seek information from them to help in their inquiries.**

119. The police appear to have been completely unaware that few of the potential victims of the crime had been alerted. When we asked AC Yates in September 2010 whether possible hacking victims had been notified, he replied: "Where we believe there is the possibility someone may have been hacked, we believe we have taken all reasonable steps with the service providers, because they have a responsibility here as well, and we think we have done all that is reasonable but we will continue to review it as we go along." In response to the question "What are these reasonable steps?" he said: "Speaking to them or ensuring the phone company has spoken to them. It is those sort of steps."[98]

120. We are reassured now that DAC Akers's investigation is setting this matter to rights by contacting all victims or potential victims. However, we were alarmed that Mr Chris Bryant MP told the House of Commons in March this year:

> When I asked Orange yesterday whether it would notify a client if their phone was hacked into now, it said it did not know. However, I understand that today it believes that in certain circumstances it might notify a client. I believe that in every such circumstance the client should be notified when there has been a problem. All that suggests a rather slapdash approach towards the security of mobile telephony.[99]

121. **We expect that this situation will be improved by the coming into force of the new Privacy and Electronic Communications Regulations, which provide that when**

98 Qq 7–9, oral evidence on Specialist Operations of 7 September 2010.

99 HC Deb, 10 March 2011, col 1171

companies discover a breach of data security, they have to notify not only the Information Commissioner but also their affected customers.[100]

122. **This inquiry has changed significantly in its remit and relevance as it has progressed, and there are further developments coming out on a regular basis. We expect that further discoveries will go beyond our current state of knowledge. Our report is based on the currently available information we have, but we accept that we may have to return to this issue in the near future.**

100 Q 156

Conclusions and recommendations

1. We have been frustrated by the confusion which has arisen from the evidence given by the CPS to us and our sister Committee. It is difficult to understand what advice was given to whom, when. Only on the last day on which we took evidence did it become clear that there had been a significant conversation between the Director of Public Prosecutions and Assistant Commissioner Yates regarding the mention in the Mulcaire papers of the name Neville and whether this and Mr Mulcaire's contract with News International were a sufficient basis on which to re-open the investigation. The fact that the CPS decided it was not, does not in any way exonerate the police from their actions during the inquiry. (Paragraph 34)

2. Section 2(7) of the Regulation of Investigatory Powers Act 2000 is particularly important and not enough attention has been paid to its significance. (Paragraph 35)

   The lack of a regulatory authority under the Regulation of Investigatory Powers Act has a number of serious consequences. Although the Information Commissioner's office provides some advice, there is no formal mechanism for either those who know they are in danger of breaking the law or those whose communications may be or have been intercepted to obtain information and advice. Moreover, the only avenue if anyone is suspected of unauthorised interception is to prosecute a criminal offence, which, as the Information Commissioner noted, is a high hurdle in terms of standard of proof as well as penalty. Especially given the apparent increase of hacking in areas such as child custody battles and matrimonial disputes, and the consequential danger of either the police being swamped or the law becoming unenforceable, there is a strong argument for introducing a more flexible approach to the regime, with the intention of allowing victims easier recourse to redress. We therefore recommend the extension of the Information Commissioner's remit to cover the provision of advice and support in relation to chapter 1 of the Regulation of Investigatory Powers Act. (Paragraph 39)

3. We also strongly recommend that the Government reviews how the Act must be amended to allow for a greater variety of penalties for offences of unlawful interception, including the option of providing for civil redress, whilst retaining the current penalty as a deterrent for serious breaches. (Paragraph 40)

4. We note that most of our witnesses claimed to be unaware at the time of the Information Commissioner's two 2006 reports, What price privacy? and What price privacy now?. We are disappointed that they did not attract more attention among the police, the media and in government, and hope that future such reports will be better attended to. (Paragraph 41)

5. We are concerned about the number of Commissioners, each responsible for different aspects of privacy. We recommend that the government consider seriously appointing one overall Commissioner, with specialists leading on each separate area. (Paragraph 42)

6. We deplore the response of News International to the original investigation into hacking. It is almost impossible to escape the conclusion voiced by Mr Clarke that they were deliberately trying to thwart a criminal investigation. We are astounded at the length of time it has taken for News International to cooperate with the police but we are appalled that this is advanced as a reason for failing to mount a robust investigation. The failure of lawbreakers to cooperate with the police is a common state of affairs. Indeed, it might be argued that a failure to cooperate might offer good reason to intensify the investigations rather than being a reason for abandoning them. None of the evidence given to us suggests that these problems were escalated for consideration by the Commissioner of the Metropolitan Police or by Ministers. The difficulties were offered to us as justifying a failure to investigate further and we saw nothing that suggested there was a real will to tackle and overcome those obstacles. We note that neither of these carefully-crafted responses is a categorical denial: Ms Brooks's denial of knowledge of hacking is limited to her time as editor of News of the World; and on payments to police, she did not say that she had no knowledge of specific payments but that she had not intended to give the impression that she had knowledge of specific cases. (Paragraph 52)

7. The consequences of the decision to focus within the Mulcaire papers on the areas vital to the prosecution of Mulcaire and Goodman were extremely significant. A huge amount of material that could have identified other perpetrators and victims was in effect set to one side. Mr Clarke explained to us the reasons for taking this approach, starting with the context at the time. By the middle of 2006 the Anti-Terrorist Branch had more than 70 live operations relating to terrorist plots but some of these were not being investigated because there were not enough officers to do so. In this context, he had to decide on priorities, and the priority of protecting life by preventing terrorist attacks was higher than that of dealing with a criminal course of conduct that involved gross breaches of privacy but no apparent threat of physical harm to the public. Nevertheless we cannot overlook the fact that the decision taken not to properly investigate led to serious wrongdoing which the Commissioner himself now accepts was disreputable. (Paragraph 55)

8. When challenged on whether he stood by his decision to limit the investigation in 2006, Mr Clarke said that, despite all that had been revealed since, he believed the decision to have been correct, given the limited resources at his disposal and the absolute priority of dealing with threats to public safety. We note this position. However, its consequences have been serious and we are not convinced that the former Commissioner's decision to merge anti-terrorist and royal protection functions on the basis that both involved firearms, or the decision to pursue this investigation within the command, were justified. It is also revealing about the nature of management within the Metropolitan Police Service that this issue does not appear to have been escalated to the Commissioner or Deputy Commissioner, or even the Assistant Commissioner, as an issue about which they ought to be aware and to which a solution needed to be found. (Paragraph 61)

9. whilst it is true that mobile phone companies have now acted to provide much greater security for their customers' communications, and whilst the 2005–07 inquiry succeeded on its own terms, we cannot say that inquiry was a success given the extent of the intrusion now becoming apparent and the fact that even now not all

the victims of interception have been identified let alone contacted. Nor are we convinced that no hacking takes places or that it cannot take place. We do not have the technical competence to make such a judgement, and nor did we receive detailed evidence on that point. (Paragraph 62)

10. Mr Hayman claims to have had little knowledge of the detail of the 2006 operation, and to have taken no part in scoping it or reviewing it; his role seems to have been merely to rubber-stamp what more junior officers did. Whilst we have no reason to question the ability and diligence of the officers on the investigation team, we do wonder what 'oversight', 'responsibility' and 'accountability'—all of which words were used by Mr Hayman to describe his role—mean in this context. (Paragraph 66)

11. Leaving aside the fact that his approach to our evidence session failed to demonstrate any sense of the public outrage at the role of the police in this scandal, we were very concerned about Mr Hayman's apparently lackadaisical attitude towards contacts with those under investigation. Even if all his social contacts with News International personnel were entirely above board, no information was exchanged and no obligations considered to have been incurred, it seems to us extraordinary that he did not realise what the public perception of such contacts would be—or, if he did realise, he did not care that confidence in the impartiality of the police could be seriously undermined. We do not expressly accuse Mr Hayman of lying to us in his evidence, but it is difficult to escape the suspicion that he deliberately prevaricated in order to mislead us. This is very serious. (Paragraph 67)

12. Mr Hayman's conduct during the investigation and during our evidence session was both unprofessional and inappropriate. The fact that even in hindsight Mr Hayman did not acknowledge this points to, at the very least, an attitude of complacency. We are very concerned that such an individual was placed in charge of anti-terrorism policing in the first place. We deplore the fact that Mr Hayman took a job with News International within two months of his resignation and less than two years after he was—purportedly—responsible for an investigation into employees of that company. It has been suggested that police officers should not be able to take employment with a company that they have been investigating, at least for a period of time. We recommend that Lord Justice Leveson explore this in his inquiry. (Paragraph 69)

13. In short, the exercises conducted by the police and the CPS in July 2009 appear to have been limited to the consideration of whether or not, in the light of recent reports in the media, the 2005–07 investigation had been carried out thoroughly and correctly. Critically, because the 2005–07 investigation had focused only on the joint roles of Messrs Mulcaire and Goodman, there was no progress in 2009 to consideration of the relationships that Mr Mulcaire might have had with other journalists, even though the Gordon Taylor story implied that such relationships had existed. (Paragraph 73)

14. We understand that, when Sir Paul announced in July 2009 that he was asking Mr Yates to look into any new information, this was an unprepared remark made as he was going into the ACPO conference rather than a carefully prepared statement. Unfortunately it left the public—and indeed Parliament—with the impression that a more detailed examination was to be held than was in fact the case. (Paragraph 80)

15. We assume that Sir Paul left Mr Yates with a large amount of discretion as to how he should consider the evidence. Mr Yates has subsequently expressed his view that his reconsideration in 2009 of the material available from the earlier investigation was very poor. We agree. Although what Mr Yates was tasked to do was not a review in the proper police use of the term, the public was allowed to form the impression that the material seized from Mr Mulcaire in 2006 was being re-examined to identify any other possible victims and perpetrators. Instead, the process was more in the nature of a check as to whether a narrowly-defined inquiry had been done properly and whether any new information was sufficient to lead to that inquiry being re-opened or a new one instigated. It is clear that the officers consulted about the earlier investigation were not asked the right questions, otherwise we assume it would have been obvious that there was the potential to identify far more possible perpetrators in the material seized from Mr Mulcaire. Whether or not this would have enabled the police to put more pressure on News International to release information, by making it clear that police inquiries were not merely a 'fishing expedition' but targeted at certain people, is an issue that may be addressed by the forthcoming public inquiry. (Paragraph 81)

16. Mr Yates has apologised to the victims of hacking who may have been let down by his not delving more deeply into the material already held by the police. We welcomed that and agree that his decision not to conduct an effective assessment of the evidence in police possession was a serious misjudgement. (Paragraph 82)

17. We are appalled at what we have learnt about the letting of the media support contract to Mr Wallis. We are particularly shocked by the approach taken by Mr Fedorcio: he said he could not remember who had suggested seeking a quote from Mr Wallis; he appears to have carried out no due diligence in any generally recognised sense of that term; he failed to answer when asked whether he knew that AC Yates was a friend of Mr Wallis; he entirely inappropriately asked Mr Yates to sound out Mr Wallis although he knew that Mr Yates had recently looked at the hacking investigation of 2005-06; and he attempted to deflect all blame on to Mr Yates when he himself was responsible for letting the contract. (Paragraph 86)

18. From the point of view of victim support and of reassurance to the public, DAC Akers's decision to contact all those who can be identified as of interest to Mr Mulcaire is the correct one. However, this is not the same as saying all these people were victims of hacking, let alone that they could be proved to be victims. Only 18 months' worth of phone data from the relevant period still exist: unless Mr Mulcaire provides a list, no one will ever know whose phone may have been hacked into outside that period. Within the 18-months data held, about 400 unique voicemail numbers were rung by Messrs Mulcaire or Goodman or from News of the World hub phones, and these are the voicemails likely to have been hacked into. The total number of people who may eventually be identified as victims of Mr Mulcaire's hacking is therefore much lower than the number of names in his papers. (Paragraph 91)

19. DAC Akers gave us a guarantee that this further investigation would be carried out thoroughly. We were impressed by her determination to undertake a full and searching investigation. The Specialist Crime Directorate is clearly the correct place

for an investigation of this sort, though we note that officers have had to be 'borrowed' from across the Metropolitan Police Service to meet the needs of this particularly labour-intensive inquiry. (Paragraph 92)

20. We note with some alarm the fact that only 170 people have as yet been informed that they may have been victims of hacking. If one adds together those identified by name, the number of landlines and the number of mobile phone numbers identified (and we accept that there may be some overlap in these), that means up to 12,800 people may have been affected all of whom will have to be notified. We accept that there are a number of reasons why progress may have been slow so far, but at this rate it would be at least a decade before everyone was informed. This timeframe is clearly absurd, but it seems to us to underline the need for more resources to be made available to DAC Akers. We understand that in the current situation of significant budget and staff reductions, this is very difficult. However, we consider that the Government should consider making extra funds available specifically for this investigation, not least because any delay in completing it will seriously delay the start of the public inquiry announced by the Prime Minister. (Paragraph 93)

21. We are seriously concerned about the allegations of payments being made to the police by the media, whether in cash, kind or the promise of future jobs. It is imperative that these are investigated as swiftly and thoroughly as possible, not only because this is the way that possible corruption should always be treated but also because of the suspicion that such payments may have had an impact on the way the Metropolitan police may have approached the whole issue of hacking. The sooner it is established whether or not undue influence was brought to bear upon police investigations between December 2005 and January 2011, the better. (Paragraph 94)

22. We are concerned about the level of social interaction which took place between senior Metropolitan Police Officers and executives at News International while investigations were or should have been being undertaken into the allegations of phone hacking carried out on behalf of the News of the world. Whilst we fully accept the necessity of interaction between officers and reporters, regardless of any ongoing police investigations senior officers ought to be mindful of how their behaviour will appear if placed under scrutiny. Recent events have damaged the reputation of the Metropolitan Police and led to the resignation of two senior police officers at a time when the security of London is paramount. (Paragraph 95)

23. We note that, despite these protections, each of the companies had identified about 40 customers whose voicemails appeared to have been accessed by Mr Mulcaire. We also note that all three companies have disciplined or dismissed employees for unauthorised disclosure of customer information in the last ten years, though there is no indication that any of these employees was linked to this case. (Paragraph 105)

24. We welcome the measures taken so far to increase the security of mobile communications. However, with hackers constantly developing new techniques and approaches, companies must remain alert. In particular, it is inevitable that companies will think it in their interest not to make using technology too difficult or fiddly for their customers, so do not give as much prominence to the need to make full use of all safety features as they should do. We would like to see security advice

given as great prominence as information about new and special features in the information provided when customers purchase new mobile communication devices. (Paragraph 111)

25. Clearly, Mr Clarke's strategy for informing victims broke down completely and very early in the process. It seems impossible now to discover what went wrong in 2006. Some of the mobile companies blamed police inaction: both Vodafone and Orange UK/T-Mobile UK said that the police had not told them to contact their customers until November 2010. AC Yates accepted that some of the correspondence between the police and the companies had not been followed up properly. (Paragraph 117)

26. However, the companies cannot escape criticism completely. Neither Vodafone nor Orange UK/T-Mobile UK showed the initiative of O2 in asking the police whether such contact would interfere with investigations (and O2 told us that they were given clearance to contact their customers only ten days or so after being informed of the existence of the investigation). Nor did either company check whether the investigation had been completed later. They handed over data to the police, Vodafone at least sent out generalised reminders about security (Orange UK/T-Mobile UK may not even have done that), they tightened their procedures, but they made no effort to contact the customers affected. (Paragraph 117)

27. We find this failure of care to their customers astonishing, not least because all the companies told us that they had good working relationships with the police on the many occasions on which the police have to seek information from them to help in their inquiries. (Paragraph 118)

28. We expect that this situation will be improved by the coming into force of the new Privacy and Electronic Communications Regulations, which provide that when companies discover a breach of data security, they have to notify not only the Information Commissioner but also their affected customers. (Paragraph 121)

29. This inquiry has changed significantly in its remit and relevance as it has progressed, and there are further developments coming out on a regular basis. We expect that further discoveries will go beyond our current state of knowledge. Our report is based on the currently available information we have, but we accept that we may have to return to this issue in the near future. This inquiry has changed significantly in its remit and relevance as it has progressed, and there are further developments coming out on a regular basis. We expect that further discoveries will go beyond our current state of knowledge. Our report is based on the currently available information we have, but we accept that we may have to return to this issue in the near future. (Paragraph 122)

Appendix 1: Excerpt from *What price privacy now?* (ICO, 2006)

Publications identified from documents seized during Operation Motorman (see para 2).

Publication	Number of transactions positively identified	Number of journalists/clients using services
Daily Mail	952	58
Sunday People	802	50
Daily Mirror	681	45
Mail on Sunday	266	33
News of the World	182	19
Sunday Mirror	143	25
Best Magazine	134	20
Evening Standard	130	1
The Observer	103	4
Daily Sport	62	4
Sunday Times	52	7
The People	37	19
Daily Express	36	7
Weekend Magazine (Daily Mail)	30	4
Sunday Express	29	8
The Sun	24	4
Closer Magazine	22	5
Sunday Sport	15	1
Night and Day (Mail on Sunday)	9	2
Sunday Business News	8	1
Daily Record	7	2
Saturday (Express)	7	1
Sunday Mirror Magazine	6	1
Real Magazine	4	1
Woman's Own	4	2
Daily Mirror Magazine	3	2
Mail in Ireland	3	1
Daily Star	2	4
Marie Claire	2	1
Personal Magazine	1	1
Sunday World	1	1

Formal Minutes

Tuesday 19 July 2011

Members present:

Rt Hon Keith Vaz, in the Chair

Nicola Blackwood	Steve McCabe
James Clappison	Rt Hon Alun Michael
Michael Ellis	Bridget Phillipson
Lorraine Fullbrook	Mark Reckless
Dr Julian Huppert	Mr David Winnick

Draft Report (*Unauthorised tapping or hacking of mobile communications*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 122 read and agreed to.

Resolved, That the Report be the Thirteenth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Tuesday 6 September at 10.30 a.m.

Witnesses

Tuesday 29 March 2011

Chris Bryant, MP

John Yates, Assistant Commissioner, Metropolitan Police

Tuesday 5 April 2011

Mr Keir Starmer QC, Director of Public Prosecutions

Tuesday 26 April 2011

Christopher Graham, Information Commissioner

Tuesday 14 June 2011

Ms Julie Steele, Head of Fraud, Risk and Security, Vodafone UK; **Mr Adrian Gorhan**, Group Head of Fraud, Security and Business Continuity, Telefonica O2; and **Mr James Blendis**, Vice President Legal, Everything Everywhere (Orange UK and T-Mobile UK)

Tuesday 12 July 2011

John Yates, Assistant Commissioner, Specialist Operations, Metropolitan Police

Mr Peter Clarke, Former Deputy Assistant Commissioner, Metropolitan Police

Mr Andy Hayman, Former Assistant Commissioner, Metropolitan Police

Sue Akers, QPM, Deputy Assistant Commissioner, Head of Operation Weeting, Metropolitan Police

Tuesday 19 July 2011

Sir Paul Stephenson, Commissioner, Metropolitan Police

Dick Fedorcio, OBE, Director of Public Affairs, Metropolitan Police

John Yates, Assistant Commissioner, Specialist Operations, Metropolitan Police

Lord Macdonald of River Glaven, former Director of Public Prosecutions

Keir Starmer, QC, Director of Public Prosecutions

Mark Lewis, Solicitor advocate, Taylor Hampton Solicitors Limited