Memorandum submitted by Amberhawk Training Ltd

Recommendation: The Committee (possibly with the assistance of the Interception of Communications Commissioner) needs to explore the consequences of the MPS legal advice (as mentioned in Q5 of Mr Yates' comments) in relation to a review of the protection afforded to individuals by the Regulation of Investigatory Powers Act 2000 (RIPA).

If the arguments underpinning the MPS legal advice, then a change to RIPA might need to be urgently recommended. When Parliament provided public authorities with intercepting powers in 1999, Parliament had in mind the protection of all messages – not just the content of the unread ones.

Argument

I refer to the evidence given by Assistant Commissioner John Yates of the Metropolitan Police Service (MPS).

Mr Yates' answer to Q5 reveals that the MPS have obtained legal advice from a leading QC which, if applied in practice, has some strange consequences. For example, it could mean that unread spam messages receive a high level of privacy protection under the Regulation of Investigatory Powers Act (RIPA) whereas read private email messages of immense confidentiality do not receive any privacy protection from RIPA.

In relation to the incidence of "voice mail hacking", Mr Yates said the following (at Q5 - see references):

> Mr Yates: ".... 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.... 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".

Note my emphasis on "prior to the owner of that voicemail intercepting it him or herself"? The question that needs to be asked is: "What does that imply?".

Consider the relevant provisions of RIPA and its definition of interception. Section 2(2) of RIPA states that "....a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if ... (he makes) ...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". Section 2(4) states that an "interception of a communication" has also to be "in the course of its transmission" by any public or private telecommunications system (my emphasis).

I had not appreciated the significance of "in the course of its transmission" or "while being transmitted" until now – but John Yates' testimony has put an end to that. What Mr Yates appears to be telling the Home Affairs Committee is that the MPS legal advice states that once the lawful recipients have read or listened to their Inbox messages, there can be no interception in connection with those messages. The RIPA offence falls away because each read message "has been transmitted" rather than "is being transmitted".

In most email Inboxes there will be all sorts of messages, some of which will no doubt left unread (e.g. spam in a "Deleted Items" folder), and some of which will be read and retained (e.g. mailings from constituents). If the MPS advice is followed, those unread spam messages gain the full protection of RIPA whereas those messages that you have read do not.

In this way, the MPS legal advice appears to imply that RIPA provides a very a topsy-turvy world of protection.

However, there is a more serious side to the MPS legal advice. If it is correct, then any claim that RIPA provides a high level of protection against the misuse of RIPA powers by law enforcement agencies could easily be misplaced. For instance, suppose the law enforcement agencies wanted to gain access to the content of an email Inbox: in relation to the content of read messages, there would be no interference, and there would be no need to obtain a warrant, because RIPA is not even engaged. RIPA's warrant provisions only cover unread messages.

It is for this reason that the arguments underpinning the MPS legal advice have to be obtained in full by the Committee. Mr Yates' comments on RIPA cannot be left to gather dust. If that advice is correct, then Parliament may need to call for a change in the law. When Parliament provided certain public authorities with intercepting powers in 1999, Parliament had in mind the content of all messages – not just the unread ones.

References: Uncorrected evidence of Assistant Commissioner John Yates: http://www.publications.parliament.uk/pa/cm201011/cmselect/cmhaff/uc441-i/uc44101.htm (begin at Q5).

September 2010

Memorandum submitted by Nick Davies, The Guardian

I am a freelance journalist. I work regularly as a special correspondent at The Guardian. I wrote the stories about the secret settlement between Gordon Taylor and News Group which were published by the Guardian on July 9 2009 and which led to new statements about the phone-hacking affair being made by Scotland Yard, the Director of Public Prosecutions and News International; and to new inquiries being opened by the Press Complaints Commission and the House of Commons select committee on media, culture and sport. Since then I have written some 30 further stories on the subject.

In relation to the three areas which you have highlighted for your current inquiry into the unauthorised hacking of mobile phones, I hope the following information may be useful.

1) **The definition of the offences relating to unauthorised tapping or hacking in RIPA and the ease of prosecuting such offences.**

i) I have written several stories which are based on paperwork which is held by the Crown Prosecution Service. This includes detailed records of phone calls, meetings and briefing papers from the original investigation by police into complaints from Buckingham Palace. Some of these records are summarised in a chronology, which was prepared by the special crime division of the CPS on July 15 2009.

The paperwork which I have read includes references to the legal advice provided by the CPS to Scotland Yard and makes no reference to Section One of RIPA requiring the prosecution to prove that an interception of voicemail has taken place before the owner of that voicemail has listened to it him or herself.

For example, following a series of exchanges in which CPS lawyers provided legal guidance to police, a briefing paper was produced on May 30 2006 by the Metropolitan Police for the Attorney General and the Director of Public Prosecutions. This referred to voicemail numbers "being accessed without authority" and to the victims of "this unauthorised access"

and goes on to suggest that "it does appear that once the telephone evidence has been secured, the police will have sufficient to arrest the potential suspects." I have read no reference to the unauthorised access needing to occur to messages which have not been read by the intended recipient.

Similarly, after David Perry QC was briefed as Crown counsel, he wrote an email on August 30 2006 to CPS lawyers in which he urged them to make a decision about the scope of the proposed indictment. He stipulated that they needed to prove that voicemail messages had actually been heard by the perpetrators but did not stipulate that they needed to prove that this had happened before the intended recipient had heard them: "The position in relation to this needs to be ascertained as soon as possible because we need to decide what the scope of the case is going to be, whether there are to be any more charges. We also need to look at the indictment to make sure the charges include the interceptions where we can prove that messages were listened to and that there is a balance between the existing three victims."

ii) I obtained a transcript of the hearing on January 26 2007 when Clive Goodman and Glenn Mulcaire pleaded guilty to offences under section one of RIPA. During this hearing, David Perry QC presented the prosecution and included (p 55ff) what he described as 'an explanation of the ingredients of the offences'. The transcript shows that Mr Perry made no reference to the notion that RIPA required the prosecution to prove that the interception had taken place before the owner of that voicemail had listened to it him or herself. Similarly, neither counsel for the two defendants nor the judge made any reference to the notion that the offence under RIPA requires this interpretation.

iii) After publication of the Guardian stories about Gordon Taylor in July 2009, the assistant commissioner for specialist operations at Scotland Yard, John Yates, made a statement on July 9 in which he made no reference to this interpretation of RIPA; and the Director of Public Prosecutions, after reviewing the case file, made a statement on July 16 in which he made no reference to this interpretation of RIPA.

iv) When reference was finally made to this by the DPP, in a memo submitted to the select committee in late July 2006, it was made clear that this interpretation of the law was something that had been mentioned in conversation at a case conference. It had never even been stated in a written opinion: "There was no written legal opinion relating to the interpretation of section 1 of the Regulation of Investigatory Powers Act 2000 (RIPA). Counsel's advice on the ambit of section 1 of RIPA was given to the CPS orally in conference."

v) The same memo from the DPP makes clear that this interpretation of RIPA has been tested in court in relation to the interception of email but not in relation to the interception of voicemail. The memo makes reference to a judgement by Lord Woolf in a case in which Suffolk police requested access to email held by NTL. Two lawyers who specialise in this area have told the Guardian with considerable confidence that that judgement does not have any impact on the use of Section One of RIPA in relation to voicemail. One of them, Simon McKay, author of Covert Policing: Law and Practice, was quoted in the paper reacting to John Yates' claim about this interpretation of RIPA: "That is nonsense and a recurring problem with the police position in this case."

Section One of RIPA stipulates that, for the offence to be committed, the interception must occur when the communication is "in the course of transmission". I understand that it is significant that whereas an old email is stored on the recipient's computer and is no longer being transmitted, an old voicemail is stored on the mobile phone company's computer with the result that whenever a voicemail is intercepted - regardless of whether its intended recipient has already heard it - that interception has to take place "in the course of transmission" from the mobile phone company's computer to the handset.

vi) Specialist lawyers add that even in the event that a court were to accept this interpretation of RIPA in relation to voicemail, the Computer Misuse Act 1998 would continue to make it an unambiguous offence to intercept voicemail regardless of whether or not it had been heard by the intended recipient. Paperwork held by the CPS shows that this act also was the subject of legal advice from CPS lawyers working with the Met police on the original investigation.

vii) It is possible that other evidence to which I have not had access will throw further light on this question. The evidence which I have seen suggests that this interpretation of Section One of RIPA is, at best, contentious; that it was not applied by police or prosecutors in the course of the original investigation and prosecution; and that it was referred to only after the Guardian put pressure on police to reconcile the version of events given in court, which disclosed only eight victims, with the emerging evidence that - in the words of the Met police briefing paper of May 30 2006 - “a vast number” of public figures had had their voicemail accessed without authority.

2) **The police response to these offences, especially the treatment of those whose communications have been intercepted.**

i) Paperwork held by the CPS shows that police began their investigation in January 2006 by analysing data held by phone companies; that this revealed "a vast number" of victims and indicated "a vast array of offending behaviour"; but that prosecutors and police agreed not to investigate all of the available leads.

In addition, the CPS paperwork shows that prosecutors were persuaded by the police to adopt a policy of 'ring-fencing' evidence so that, even within the scope of the limited investigation, there would be a further limit on the public use of evidence in order to ensure that 'sensitive victims' would not be named in court. This appears to have referred to a policy of not naming members of the royal family whose messages had been intercepted. It is not clear whether the ring-fencing extended to the suppression of the names of other potential victims such as senior officers at Scotland Yard.

On August 8 2006, police arrested Clive Goodman, Glenn Mulcaire and one other man who was not finally charged. They seized computer records, paperwork, audio tapes and other material from all three men. As a result of an application by the Guardian under the Freedom of Information Act in January 2010, we now know that this material included 4,332 names or partial names of people in whom the men had an interest; 2,978 mobile phone numbers; 30 audio tapes which appear to contain recordings of voicemail messages; and 91 PIN codes of a kind which are needed to access mobile phone messages in the minority of cases where the owner has changed the factory settings on their mobile phone.

It has now become clear that, having seized this material, police chose to impose a further limit on their investigation by not fully searching and analysing it. This job was finally done only in the aftermath of the Guardian stories in July 2009. This emerged in written evidence to the media select committee in February 2010 after the Guardian disclosed the fact that the seized material contained 91 PIN codes. The chairman of the select committee, John Whittingdale, wrote to the assistant commissioner, John Yates, to complain that he had not mentioned this when he gave oral evidence to the committee in September 2009. Mr Yates replied that "the specific figure supplied in the FoIA request on January 28 2010 was not available at the time I came before your committee in September 2009."

Further evidence of the decision not to fully search and analyse the seized material also appears in a memo written to government ministers by Mr Yates' staff officer, Det Supt Dean Haydon, on February 18 2010 in which he stated that "minimal work was done on the vast personal data where no criminal offences were apparent".

ii) The decision not to investigate all the leads in the phone data and the subsequent decision not to fully search and analyse the seized material meant that there was a failure to investigate all those who may have been involved in associated criminal activity.

Police chose not to seek a production order requiring the News of the World to disclose internal records. Instead, as evidence to the media select committee disclosed, they wrote a letter to the newspaper asking them for disclosure of a list of items. The newspaper refused to comply, and Scotland Yard accepted this without further action.

Police also chose not to interview any reporter, editor or manager at the newspaper other than Clive Goodman. Emerging evidence about the phone data and other material in the possession of the police reveals that they were in possession of evidence which implicated named employees of the News of the World in dealing with the interception of voicemail messages. It is not clear whether police knew that they had this evidence and chose not to pursue it; or whether their decision not to fully search and analyse the seized material meant that they were unaware of it.

Among this material was an email, sent in June 2005, by a reporter in the News of the World's newsroom to Glenn Mulcaire for the attention of the newspaper's chief reporter, Neville Thurlbeck. This email contained transcripts of some 35 voicemail messages taken from the phones of Gordon Taylor, chief executive of the Professional Footballers Association, and of Jo Armstrong, his legal adviser. Responding to questions from the Guardian in July 2009, the DPP disclosed that police had never passed this document to prosecutors, even though Gordon Taylor was one of the eight victims named in the indictment. The DPP and police have said that crown counsel 'had access' to all undisclosed material held by police. It is not clear, however, that crown counsel actually ever saw this document. The seized material was so complex and voluminous that it took Scotland Yard officers several months to search it when finally they undertook the task in July 2009. Responding to the Guardian's inquiry, the DPP conceded that crown counsel does not remember seeing it: “He cannot now recall whether the email was the subject of specific advice at the time."

iii) The same decisions which limited the original police investigation of possible offenders also meant that there was a failure to investigate all those who were, or who may have been, victims of voicemail interception.

In terms of the prosecution, this meant that the case was presented on the footing that there were only eight victims. No offences involving other victims were presented to be 'taken into consideration' by the court. Nor were any further offences involving other victims 'left on the file'. Nothing that was said in court or in any public statement by police or prosecutors at the time of the trial indicated that the eight named victims were only a representative sample of a “vast number” of public figures whose voicemail had been accessed without authority.

Separately, there is an issue about the warning of those who were or who may have been victims. In a statement on July 16 2009, following the Guardian's stories, the DPP disclosed for the first time that the eight named victims had been only a representative sample and added: "For any potential victim not reflected in the charges actually brought, it was agreed that the police would inform them of the situation."
In written evidence to the media select committee in February 2010, John Yates suggested that this was indeed what police had done: "What we can say is that where information exists to suggest some form of interception of an individual's phone was or may have been attempted by Goodman and Mulcaire, the MPS has been diligent and taken all proper steps to ensure those individuals have been informed."

However, the emerging evidence suggests that Scotland Yard have failed to honour their agreement with the DPP to inform "any potential victim":

a) There are examples of their failing to inform people at the time of the original investigation even though they were holding clear evidence that Mulcaire had succeeded in intercepting their voicemail. This was conceded in evidence to the media select committee in July 2009 when John Yates said that following publication of the Guardian stories in July 2009, police had informed a small number of victims who had not previously been approached. Even then, however, they failed to complete the task in relation to these confirmed victims. In the case of Jo Armstrong, for example, they had the email of June 2005 which included transcripts of messages taken from her phone. The media select committee asked John Yates when Jo Armstrong was informed. In December 2009, Mr Yates wrote in reply: "Ms Armstrong was not one of the victims selected or named in the indictment to highlight the breadth and scale of those targeted by Mulcaire and Goodman and was therefore never spoken to by the MPS." Scotland Yard continue to refuse to say how many victims were warned at the time of the original investigation and how many have been warned since publication of the Guardian stories in July 2009.

b) A further group of confirmed victims was identified by three of the five mobile phone companies but, contrary to the police agreement with the DPP, many of them were not informed. At the time of the original investigation, Scotland Yard passed Orange, Vodafone and O2 details of the phone numbers being used by Goodman and Mulcaire so that the three companies could search the data which they hold for a rolling twelve-month period in order to try to identify customers whose voicemail had been accessed from those numbers. In February 2010, the Guardian discovered that each of the companies had identified approximately 40 victims; that Orange had warned none of them; Vodafone had warned them 'as appropriate'; and only O2 had a policy of warning all of them. Correspondence from Scotland Yard suggests that they were unaware of the identification of these victims and had made no attempt to ensure that all of them had been informed. It is not clear why Scotland Yard did not also involve the other mobile phone companies in this exercise.

c) Among 'potential victims', where the evidence of successful interception was not so clear, there is evidence of the police engaging in a limited attempt to honour their agreement with the DPP. In written evidence to the media select committee in September 2009, Mr Yates stated that "police led on informing anyone who they believed fell into the category of Government, Military, Police or Royal Household if we had reason to believe that the suspects had attempted to ring their voicemail. This was done on the basis of national security." Scotland Yard continue to refuse to say how many people were approached in each of these four categories.

d) Another group of potential victims appears to have been given less attention. We now know that police found in the seized material 91 PIN codes of a kind needed to intercept voicemail from those targets who have changed the factory settings on their phones. Although the owners of these PIN codes would appear to qualify as 'potential victims', they were not all informed. For example, the actor Sienna Miller, through her lawyer, has disclosed that her PIN code was found in Mulcaire's possession together with her mobile phone number and that Scotland Yard did not inform her until her lawyer wrote a series of letters requesting the information.

e) There is a further category of an unknown number of people whose names and mobile phone numbers and/or other personal data were found in material seized from Mulcaire. These mobile numbers were found in the possession of a private investigator who was specialising in the interception of voicemail messages for a newspaper; the owners of these numbers are public figures; they are the subject of news coverage; they are not the personal acquaintances of Mr Mulcaire; their numbers and other details were found in his work records, not in some personal address book. The police concluded that they were not 'potential victims' and informed none of them. Chris Bryant MP is an example in this category.

f) There is a final category of people whose names were found on invoices recording payments claimed from the News of the World by Mulcaire. The then deputy prime minister, John Prescott, is one of these. He was named on two invoices in the Spring of 2006. Even though Mr Prescott was then in a very senior position in government which meant that he was involved in current matters of defence and counter-terrorism and was in receipt of sensitive political and economic information, police did not approach him to inform him that he had been targetted by a private investigator who specialised in the interception of voicemail messages.

The apparent failure to honour the agreement with the DPP has had some practical results for those victim and potential victims who received no warning. Because mobile phone companies are allowed to hold call data for only 12 months, these people have lost the chance to check to see if anybody had accessed their messages and, if so, who that might be. They had no chance to change their PIN codes to make their messages secure for the future and no opportunity to assess what confidential messages might have been heard.

Following the Guardian stories in July 2009, John Yates ordered officers at Scotland Yard to fully search and analyse the material seized nearly three years earlier, in August 2006. That search led to the creation of a spreadsheet which lists all those named in the seized material together with a summary of the personal information held on them. Scotland Yard chose not to publicise the existence of that spreadsheet and, shortly after it was finally created, at a media briefing in November 2009, a senior officer attempted to deny that it existed and conceded that it did exist only when confronted with detail about it.

Since then lawyers who have contacted Scotland Yard on behalf of clients report that they have received letters which have failed to give them a clear summary of the material relating to them which is in the possesion of the police. I have spoken to several representatives of public figures who were simply misled by the wording of Scotland Yard's letters which led them wrongly to believe they had not been targeted by Mulcaire.

3) **Police action to control these offences**

The original police inquiry was highly effective in uncovering the truth about the interception of voicemail in the royal household. The jailing of a Fleet Street journalist sent a powerful message to the profession, that this practice was not only unlawful but also dangerous. It is reasonable to conclude that this must have had an impact in reducing the use of illegal techniques in newsrooms.

However, there is evidence that some in Fleet Street have continued to use illegal techniques, including the interception of voicemail. It is reasonable to conclude that the limiting of the original police inquiry sent a contradictory message to those journalists who had been involved in illegal techniques, suggesting that the police had only a limited interest in uncovering these offences.

The evidence suggests that the police continue to take an equivocal approach to enforcing the law in Fleet Street. Scotland Yard have insisted that they will not investigate the mass of unused evidence which they have held since 2006 – the unfollowed leads on the “vast number” of victims found by analysing phone data by May 2006; and the information about potential offenders and potential victims in the material seized from suspects in August 2006.

Instead, they have said they will investigate only “new evidence”. And in this, it appears that they have restricted themselves to new evidence which is placed in the public domain by news organisations. For example, they agreed to interview Sean Hoare, who was named in the New York Times as a witness who alleged that the former editor of the News of the

World, Andy Coulson, had encouraged the interception of voicemail; and Paul McMullan, who was named in the Guardian as a witness who alleged that Andy Coulson must have known about the widespread use of illegal techniques at the newspaper.

However, they have not attempted to find their own “new” witnesses and chose to tell their short list of witnesses provided by the media that they must be interviewed 'under caution', ie on the basis that anything they said might be used to prosecute them. Sean Hoare declined to comment on important questions. Paul McMullan refused to co-operate voluntarily with an interview on that basis.

October 2010

Memorandum submitted by Mark Lewis, Taylor Hampton Solicitors

By way of background, I was the Solicitor who acted for Gordon Taylor, Joanne Armstrong and another whilst at my previous firm. I gave evidence to the Select Committee in the last Parliament that amongst other things looked at press standards. I am currently representing other victims of phone-hacking.

I have also instituted libel proceedings in my own right against the Press Complaints Commission ("PCC"), Baroness Buscombe (the PCC's chair), and the Metropolitan Police Service ("the Met") as a result of publications made by them about my evidence to the aforementioned Select Committee. In a speech to the Society of Editors Baroness Buscombe made reference to my evidence saying that I had misled Parliament. I stand by my previous evidence and repeat it.

On the last occasion I gave evidence as to the statement made to me by DS Maberley (now DI) outside Court at a hearing seeking disclosure from the Met. My evidence was that he told me that there were "6000 victims" of phone hacking.

The issues that arise from my dealings are:

1. The actions of the Met; and
2. The actions of the News of the World.

THE MET

1.1 RIPA
1.2 Notifying victims
1.3 Misleading letters
1.4 Public statements

1.1 RIPA

1.1.1 The Met rely upon a definition of the phone hacking crime, as being an offence under RIPA. The Met say that unless it is possible to prove that the offender listened into a voicemail of another and heard a message before the intended recipient, then there is no crime.

1.1.2 It follows that if an offender listens into another person's voicemail, by surreptitious means, the determination as to whether a crime has occurred is based upon whether the message is a new message or a saved message. That distinction does not make any sense. The message is the same in either case, the conduct of the person listening to the message is the same in either case, and the timing might be a second apart.

1.1.3 The narrow definition of the RIPA crime seems to be used to justify the Met's failure to notify victims of crime. If listening to a saved message is not a crime then the victim of phone hacking is not a victim of a crime under RIPA.

1.1.4 The Met has not indicated whether it has considered any other offence (if they are correct under RIPA) such as the Computer Misuse Act or any crimes of attempt. The Met has not revealed whether it is aware that other people (whose phones were hacked), had listened to their messages before the hacker. If they do not know that was the case then the public statements and letters from the Met are misleading (see below).

1.2 NOTIFYING VICTIMS

1.2.1 The decision to notify victims was arbitrary. When Glenn Mulcaire was prosecuted, the Met notified a few victims but not others. Mr Mulcaire was prosecuted for hacking Gordon Taylor, Max Clifford, Simon Hughes MP, Elle McPherson and Skylet Andrew as well as the members of the Royal Household.

1.2.2 I gave evidence to the last select committee about Gordon Taylor and Joanne Armstrong (the first two civil cases). Mr Taylor was notified by the Met. Ms Armstrong was not. There was no difference between the offences against either. Both had their phone hacked.

1.2.3 I am aware of other situations where one person was told but another in the same building was not. The Court records show that I am acting for (amongst others) Nicola Phillips who worked with Max Clifford.

1.2.4 There is no doubt that the Met were aware of Ms Phillips as the documents given to Mr Clifford included documents about her. The same situation happened where Gordon Taylor was notified by the Met but Joanne Armstrong was not. Others within the football world were not notified even where their details must have been held by the Met.

1.2.5 Even now, the Met refuses to hand documents to victims without a Court Order. Matters are made worse as the same documents were given to third parties who had less right to see them. For example, Max Clifford (according to the Court papers in his case) was told by the Met that Nicola Phillips phone had been hacked but she was not told.

1.2.6 Statements made by the Met that they are notifying victims depend upon their narrow definition of RIPA. The "victims" that I represent have not been told.

1.3 MISLEADING LETTERS

1.3.1 The Met approach to requests from potential victims seems deliberately obstructive. Any request is met by a series of letters:

1.3.1.1 A request for a letter of authority from the client;

1.3.1.2 An acknowledgement that a search is being made (often after a reminder and a long delay);

1.3.1.3 It is made clear by the Met that even if the search reveals any information it will not be released without a Court Order as the documents were seized for the purpose of a criminal investigation. (Note that if the person had been invited to be a prosecution witness then they would have seen the documents without such an Order).

1.3.1A It seems incredibly obtuse to refuse to tell a victim of crime that they cannot have the evidence of that crime.

1.3.1.5 Finally, usually after 2-3 months a person who was a victim of Mulcaire gets a letter that includes an opening paragraph to the effect of "you were a person of interest to Mr Mulcaire. During our search we found a list with your name on it X times, your phone number Y times. Letters might also add that your name was found in an email, and that a billing guide shows that there were calls from people who had a "connection with News of the World". There is no explanation as to why the Met chose to take no action against the people that they describe as such people connected to the News of the World and how they were connected.

1.3.2 The standard letters conclude with the phrase "there is no evidence to show that you were a target of Mr Mulcaire". Phrases to that effect can only be designed to put off those who have made the inquiry or their solicitors. Quite plainly, there is evidence but not proof. It is the lawyer's job to garner the evidence and make the case. Individuals who see that phrase are put off by thinking that the lack of evidence asserted by the Met is relevant. The phrase used by the Met would have the same meaning if expressed negatively "there is no evidence to show that you were not a target of Mr Mulcaire." The Met has no business volunteering any advice. It seems clear that such advice is deliberately designed to stop people taking further action against the News of the World.

1.4 MISLEADING STATEMENTS

1.4.1 The Police and former police officers have made public statements which have the effect of misleading the public and thereby putting them off bringing a claim.

1.4.2 The initial investigation was undertaken by Andy Hayman ("Mr Haymann") 'who has now left the Met. Mr Hayman is now employed by News International as a columnist (or one of its subsidiaries). Mr Hayman is on record referring to a "handful of victims" of phone hacking, using his supposed insider's knowledge to exonerate his new employers. There is an unhealthy position that a former Police Officer who must be bound by the Official Secrets Act feels able to discuss operational matters that occurred during his service within a newspaper published by the party he was meant to investigate. If permission has been given by the Met to reveal operational secrets then that must be said. If not, then action must be taken against Mr Hayman.

1.4.3 Assistant Commissioner Yates holds that line. The latest public statement by the Assistant Commissioner is that there were" 10-12 high profile victims". That seems to be based upon a vague definition of "high profile" (the profile of a victim of crime should be irrelevant) and the narrow definition of "victim" used by the Met.

1.4.4 It is not clear why the Met have chosen not to act openly. The impression created by the former investigating officer, now working for the organisation that was investigated is extremely alarming. Assistant Commissioner Yates has now conceded that Neville Thurlbeck should have been interviewed during the initial investigation. The Met operation that decided not to investigate Mr Thurlbeck was headed by Mr Hayman. Mr Hayman and Mr Thurlbeck are now colleagues.

1.4.5 The statement that seeks to explain the position is "there is no new evidence". That might be so. The issue has always been that evidence existed but was not used. It is disconcerting that the Met's failure to use that evidence is being investigated by the Met. There can be no confidence in a situation whereby the Met investigation of an incident can result in a criticism of the Met. That is obviously a conflict of interest as the Met is best served by a finding that shows it acted properly in the first place.

1.4.6 There are all sorts of explanations as to why the Met might have failed to investigate Properly

1.4.6.1 The initial investigation related to the Royal household. For that reason the investigation was allocated to a particular team. When it became clear that the investigation was much wider, the inquiry should have been transferred to a bigger team that had appropriate resources;

1.4.6.2 Former Met Officers go to work for News International after retirement (the parent company of News Group Newspapers) such as Mr Hayman. There should not be such an incentive. It is difficult to see whether Mr Hayman would have been appointed if he had extended the scope of the investigation and prosecuted further.

1.4.6.3 News of the World investigations are passed to the Met. It follows that the Met might themselves use information that derives from phone hacking. That has to be a disincentive to a thorough investigation by the Met;

1.4.6.4 The News of the World and other media often accompany the Met to see secret arrests. The alliance between the News of the World and the Met has the appearance of being too close and might be too close.

1.4.6.5 At the relevant time, Mr Hayman had reason to fear that he was a target of Glenn Mulcaire and the News of the World. It became public knowledge that throughout the period of the investigation into voicemail hacking, Mr Hayman was involved in a controversial relationship with a woman who worked for the Independent Police Complaints Commission and was claiming expenses which were subsequently regarded as unusually high.

1.4.6.6 The same, of course, is also true of John Yates who, we now know, at the time when he responded to the Guardian stories about Gordon Taylor's settlement with News Group was involved in a controversial relationship with a woman who worked for the Met press bureau.

1.4.6.7 At the time of the Guardian story a statement was rushed out by the Met with indecent haste. Although it seems far fetched that the News of the World would have hacked into phones of Police Officers, we now know that Mr Brian Paddick's phone was hacked and he was not notified by the Met that they had such information.

1.4.6.8 The Met were just incompetent and failed to realise the importance of the documents that they had.

1.4.6.9 The Met were under-resourced and therefore failed to read the documents.

1.4.7 The above are not materially inconsistent so 2 or more of the explanations might be valid together.

NEWS OF THE WORLD

2.1 Until there is a proper and thorough investigation of the papers held by the Met, the extent of unlawfulness by the News of the World will not be known. The investigation by the Met is unlikely to conclude with a decision that leads to criticism of their initial investigation or charges against their own officers (if there was a deliberate decision not to interview or prosecute offenders).

2.2 Without such an investigation it will not be known who should be prosecuted.

CONCLUSION

I am willing to give evidence to the Home Affairs Select Committee in order (0 amplify any of the above submissions.

October 2010

Memorandum submitted by the Information Commissioner's Office

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000. The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The Commissioner's response to this consultation is primarily based on the practical experience the ICO has gained in regulating compliance with the DPA.

2. As Information Commissioner, I welcome the opportunity to contribute to the Home Affairs Committee inquiry. I should point out at the outset that it is important to recognise the context of the legislative framework within which hacking and tapping are regulated, and the very limited role I have as Information Commissioner in the oversight of the interception of communications**.**

3. In my role as Information Commissioner, I have been involved in the debate about the unlawful trade in personal information. The most high profile case my office has dealt with in this area was Operation Motorman.[1] This was a case where a private investigator had been supplying personal information to some 305 journalists. The personal information included details of criminal records, registered keepers of vehicles, driving licence details, ex-directory telephone numbers, itemised telephone billing and mobile phone records. Documentation seized at the home of the private investigator included reports, invoices, settlement of bills between the detective and many of the better known national newspapers - tabloid and broadsheet. The case touched upon similar issues to those raised by the interception of communications, but this was not the main focus of the investigation; nor am I, as Information Commissioner, empowered to investigate or act on unlawful interceptions.

4. As Information Commissioner, I have oversight of the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Thus I have responsibility for taking action on the DPA s.55 offence that may arise from the unlawful 'blagging' of personal information from a data controller. 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 (RIPA). This means that the regulatory regime that covers the use, disclosure and interception of communications related data is fragmented.

5. My office has direct experience of dealing with some of the complaints that arise under the current mosaic of regimes that govern the various forms of communications data processing in the UK. In particular, cases come to my office about processing of communications data which have been collected through interception of communications.

[1] Operation Motorman was the subject of two reports to Parliament by the Information Commissioner, published as *What Price Privacy? May2006* and *What Price Privacy Now? December 2006*

6. The first data protection principle states that processing of personal information must be fair and lawful. Any processing of personal information which has been obtained In contravention of the provisions of section 1(1) of RIPA would also be in breach of the first principle. Understandably organisations approach the ICO for advice. However, it is inappropriate and arguably beyond the powers of the Information Commissioner to advise on the lawfulness of interceptions of communications under RIPA. My office does not have particular expertise or regulatory competence in this area. An organisation could follow the advice of my office but still be liable for prosecution if the prosecuting authority for RIPA takes a different view.

7. Section 57 of RIPA creates the role of Interception of Communications Commissioner, but his role is limited to overseeing the persons who issue warrants, and the procedures of those who are acting under warrant or who are assisting those acting under warrant. RIPA places no duty on the Interception of Communications Commissioner to provide advice to those who are not covered by RIPA, mostly private sector actors, who want to ensure they are acting in a manner which is in compliance with RIPA, nor is he resourced to provide such advice.

8. The Interception of Communications Commissioner has no remit to investigate complaints about those bodies outside RIPA who have contravened the requirements for "lawful interception" of communications. This also applies to the Investigatory Powers Tribunal. Effectively, what this means is that where the private sector, either through their own provision of services, or through being placed under a legal obligation, are intercepting communications of service users, there are gaps in the regulatory regime. The only recourse for a private sector breach is prosecution for a criminal offence. This is a very high bar, and on many occasions the nature of the offence and harm committed by the offence may not justify a criminal prosecution, but still justify some form regulatory action, which neither body is empowered to take. This is different from the position that applies to the public sector, where there is regulatory oversight of interception of communication.

9. Under the Data Protection Act, when my office is approached for advice as to the application and applicability of data protection law, the Information Commissioner is empowered to provide such advice under section 51 of the Data Protection Act 1998. Indeed, the Information Commissioner is under a specific obligation to promote the following of good practice which includes but is not confined to compliance with the requirements of data protection law. The problem is that whilst the DPA, PECR and RIPA together form part of the framework of regulation that limits excessive surveillance and provides safeguards for individuals, it is only in relation to the DPA and PECR that there is an organisation charged with promoting compliance with the legislation and with providing authoritative advice to those who need it.

10. As Information Commissioner, I have made it clear on several occasions that there is a great difficulty with the gaps in the current regulatory regime covering interception of communications. It is important that individuals are given adequate protection in this ever evolving area. This is of particular interest at present, as the UK is facing potential infraction proceedings in the European Court of Justice as a result of the way in which the UK has implemented the EU Privacy Directive's provisions on interception of communications. My office has been assisting Government in responding to these proceedings.

October 2010

Memorandum submitted by Keir Starmer QC, Director of Public Prosecutions

Thank you for your letter of 7 October 2010 seeking my views on the definition of offences relating to unauthorised tapping or hacking of mobile communications and, in particular, whether the relevant statutes present difficulties in terms of gathering sufficient evidence to prosecute a case. I am, of course, happy to assist you and the Committee and, to that end, I will deal first with the relevant law; then with the approach taken in the widely-reported prosecution of Clive Goodman and Glen Mulcaire in 2006; and finally with the general approach that I intend to take in relation to on-going investigations and future investigations.

The relevant law

The relevant law is complex. 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.

As is well known, Part I of RIPA deals with communications generally. Chapter 1 (sections 1-20) deals with "Interception", the provisions of sections 1-5 setting out the framework and definitions for lawful, unlawful and authorised interception.

Section 1 creates two interception offences. Section 1(1) of the Act provides:

> "(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) ...; or
>
> (b) a public telecommunication system. "

Section 1(2) creates a like interception offence in respect of private telecommunication systems, which excepts from liability the system controller or someone acting with the consent of the user. This is a considerable extension of the previous statutory regime.

The Act defines 'communication' (section 81(1)) as including

> "(b) anything comprising speech, music, sounds, visual images or data of any description; and
>
> (c) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;"

When considering what hardware is comprised in the system over which the communication is transmitted, 'apparatus' is defined in section 81(1) as including any equipment, machinery or device and any wire or cable.

There are then both geographical and 'system' limits to liability for the offence of unlawful interception under section 1 - the interception must take place in the United Kingdom and it must occur in the course of transmission by a public or a private telecommunication system (a private system is a telecommunications system directly or indirectly attached to a public one). Once the communication can no longer be said to be in the course of transmission by means of the 'system' in question, then no interception offence is possible.

The central core of the actus reus of the offence requires proof that a communication was intercepted. As to what is interception, section 2(2) provides as follows:

"(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 telecommunications 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."

Meaning of 'modifies', section 81(1) provides that "modification" includes alterations, additions and omissions, and that cognate expressions shall be construed accordingly; its meaning in section 2 is also further dealt with by subsection (6).

"Interferes" is not further defined and neither is the word "monitors"; however, the ordinary meaning of the word "monitors" includes "listen to and report" and "observe" (New Shorter Oxford Dictionary, 2002). It is thus wide enough to include listening in to a telephone conversation or to a unilateral telephone speech message.

As to any limit of time in the definition of unlawful interception, section 1 contains the expression '...in the course of its transmission...'; section 2(2), which defines interception, refers again to this expression and also contains the words 'while being transmitted. This confinement of the time window for unlawful interception is further reflected in subsection 2(8). 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. However, it should be noted that the limiting definition of interception in section 2(2) is expressly made subject to the other provisions of section 2 that follow (i.e. subsections 2(3)-(11)). They deal with such matters as broadcast transmissions, territoriality, and the distinction between communication content and attached traffic data among others.

Of most significance to you and the Committee is the fact that the definition of interception in subsection 2(2) is to be read subject to the particular provision in subsection 2(7), which extends the concept of transmission, and with it the time window, and reads as follows:

"(7) For the purposes of this section the times while a communication is . being transmitted by means of a telecommunications 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."

The specific extension of both the times and the kind of activity taking place during which a communication is being 'transmitted' therefore includes any period during which the transmission system stores the communication; but it does not extend to all such storage, but only those periods when the system is used for storage "in a manner that enables the intended recipient to collect it or otherwise to have access to if'.

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?

Unfortunately there is no decision yet in which a court has determined this construction issue.

Some assistance can be gleaned from a series of decisions in which the Court of Appeal has considered the definition of interception. Most of these cases have been in the context of telephone voice communications, where investigators used equipment to record speech associated with the call which was then sought to be adduced as evidence for the Crown: see, for example, *R. v. Hardy & Hardy* [2003] 1 Cr. App. R. 494 and *R. v. E.* [2004] 2 Cr. App. R. 484 (and the other authorities referred to by the Court of Appeal in giving its judgment). If there is a theme, it has been to restrict the ambit of the interception definition in this context.

Perhaps the case most on point so far is R. *(on the application of NTL GroupLtd.) v. Ipswich Crown Court and another* [2002] 3 W.L.R. 1173, [2003] Q.B. 131, [2002] EWHC 1585 (Admin.)., where the Divisional Court considered the situation of a telecommunications company facing an application for the production of the content of e-mails said to be relevant to a fraud investigation, by police officers who had applied to the Crown Court under section 9 and Schedule 1 of the Police and Criminal Evidence Act 1984. The company argued that if the order made applied to material in the system before it was made, it might well find itself in breach of section 1(1) of RIPA, having regard to the provisions of section 2(7) & (8). The Court held that, subject to authorisation by the making of the order, the company would have committed the section 1 offence, since diverting the content of the mails to storage and so making them available would amount to interception. In his judgment Lord Woolf CJ observed at paragraphs 18-19 that in relation to the effect of section 2(7) of RIPA: 'Subsection (7) has the effect of extending the time of communication until the intended recipient has collected it'.

In due course, no doubt, the proper construction of sections 2(2) and 2(7) of RIPA will be determined authoritatively by a court. 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 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 Glen Mulcaire in 2006; and then indicate the general approach that I intend to take to on-going investigations and future investigations.

The prosecution of Clive Goodman and Glen Mulcaire

Both Clive Goodman and Glen Mulcaire pleaded guilty before the Central Criminal Court on 29 November 2006 to one count of conspiracy to intercept communications in respect of voicemail messages left for members of the Royal Household. Mulcaire alone pleaded guilty to five further substantive counts in respect of Max Clifford, Andrew Skylet, Gordon Taylor, Simon Hughes and Elle MacPherson. On 26 January 2007, Goodman was sentenced to four months' imprisonment and Mulcaire to a total of six months' imprisonment, with a confiscation order made against him in the sum of £12, 300.

In the course of those proceedings, no challenge was made to the prosecution case and the judge was not required to make any ruling on the legal definition of any aspect of RIPA.

I was not in post as DPP at the time of the prosecution of Clive Goodman and Glen Mulcaire, and therefore have no first hand knowledge of the way in which it was prosecuted. Moreover, the CPS lawyer dealing with the case at the time has now left the CPS. However, in 2009 I discussed the case with David Perry QC, who was instructed as leading counsel at the time, and with my predecessor, Lord Macdonald of River Glaven. It is my understanding that David Perry QC gave oral advice about the interpretation of sections 1 and 2 of RIPA at the time. He advised that, for the purposes of prosecuting Clive Goodman and Glen Mulcaire, if it became an issue, the prosecution may have to consider taking a narrow view of the offences under section 1(1) of RIPA. This was a case specific decision.

However, as matters turned out, it was not necessary to resolve in the proceedings whether section 1(1) of RIPA required proof that the interceptions had taken place before the intended recipients had listened to the messages. There were two reasons for this. First, the prosecution did not in its charges or presentation of the facts attach any legal significance to the distinction between messages which had been listened to and messages which had not. Secondly, the prosecution not having made the distinction, the defence did not raise any legal arguments in respect of the issue, and pleaded guilty. It is evident, therefore, that the prosecution's approach to section 1(1) of RIPA hadno bearing on the charges brought against the defendants or the legal proceedings generally. Indeed, the prosecution was not even required to articulate any approach. The issue simply did not arise for determination in that case.

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.

On-going and future investigations

Obviously the approach taken in the prosecution of Clive Goodman and Glen Mulcaire was case specific and the advice of David Perry QC has to be seen in that context. The approach in any given case will, in the end, depend on the facts in issue. But, on a much more general basis, 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 beinhibited 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.

I hope that this, unavoidably lengthy and technical, explanation of the difficulties of interpreting the relevant provisions of RIPA is helpful. I emphasise, once again, that providing a definitive interpretation of the law is ultimately for the court not me.

In view of my previous correspondence to the Culture, Media and Sport Committee, I am copying this letter to John Whittingdale MP.

October 2010

Memorandum submitted by Paul McMullan

Further to our conversation today a brief email to explain phone hacking was very easy in the 90s when people were new to mobiles and did not change their codes, you simply rang them up to ensure their phone was engaged; you rang a second time, got to their message system pressed 9, followed by 0000, you could then listen to all their messages. Everyone in the schoolyard did it, many particularly showbiz journos did it. It wasn't particularly illegal. For what it is worth Andy Coulson knew a lot of people did it at The Sun on his bizarre column and after that at NOTW. As he sat a few feet from me in the newsroom he probably heard me doing it, laughing about it etc and told others to do it. I worked under Coulson for a year and a half at NOTW. The real scandal is Cameron would have been briefed: "We can probably get away with this one," when hiring Coulson, so Mr Cameron is either a liar or an idiot. Hacking got more difficult as time progressed with call waiting so it was more difficult to provoke an engaged tone and by around 2006, actually probably after if not because of the Clive Goodman trial many mobile networks would not let you have a message system unless you put in your unique code. However people who worked for Vodaphone etc would sometimes ring up the news desk offering to sell numbers and codes of stars' phones, as indeed did people at the tax office, people in doctors receptions etc. That is your real problem. As you make phones more difficult to hack so you increase the value of an insider's information. You can also scan/intercept mobile phones but the equipment is expensive to keep up to date with, if I can be of any further assistance feel free to email or call **********, and leave a message, boom boom. In truth I never got a decent story from hacking messages. If people have something important to say they say it to the person when he picks up. It was a third rate trick used by school kids and third rate journalists. There is no real security risk and more fool the MP who leaves messages about nuclear secrets etc. Scanning is another issue but you will have to ask your security peeps about protecting your phone from that, regards Paul

November 2010

Memorandum submitted by Everything Everywhere

Background

1. Everything Everywhere is the newly created company formed by the merger on 1 April 2010 of the mobile and broadband communications companies Orange UK and T-Mobile UK.

2. It is a 50:50 joint venture between France Telecom and Deutsche Telecom, the owners of the respective Orange and T-Mobile global businesses. The Everything Everywhere joint venture applies only to their UK businesses and they therefore remain entirely separate and competing companies throughout the rest of the European Union (and the world).

3. Everything Everywhere is an independent business operating at arms-length from France Telecom and Deutsche Telecom, although their representatives sit on its board. The views expressed in this submission do not therefore reflect the views of France Telecom or Deutsche Telecom.

4. Despite the merger, the Orange and T-Mobile brands continue to co-exist and 'compete' in the UK market. But the views expressed in this submission do reflect the combined views of Orange and T-Mobile in the UK.

5. Through its Orange and T-Mobile brands, Everything Everywhere principally provides mobile voice and internet/data services to nearly 30 million UK consumers. In addition, it also provides landline broadband and voice telephony through the Orange brand and WiFi internet access through the T-Mobile brand.

6. Our voicemail service has been designed to enable customers to access their mailboxes both from their own mobile phones and from other phones. We find that customers appreciate this service, as it allows them to listen to stored messages, or to change the greeting on their mailbox, regardless of whether they use their own phone.

How widespread is the problem of unauthorised tapping or hacking?

7. We have no evidence to support the contention that the practice of unlawfully accessing mobile voicemails is widespread. Our customer service contact centres deal with over a million enquiries each week, and the reasons for their calls are carefully monitored so that emerging issues can be identified and addressed before they reach a critical mass and have an adverse impact on other customers.

8. The level of enquiries that are received from people who are concerned about the security of their voicemail accounts is so low that statistics are simply not kept. If this issue ever were to be of general concern, a "reason code" for the call would be created, which would enable the business to monitor the volume of enquiries more precisely, and address the matters that would be raised.

What are we doing to monitor and prevent unauthorised tapping?

9. Our voicemail platforms incorporate a range of security features which provide an appropriate level of protection against all but the most determined hacker.

10. We do not disclose full details of network features that protect voicemail services, but we continually review security features to protect against new and emerging threats. Protective measures include:

    - Provisioning mailboxes with a random PIN;
    - Preventing users from changing the random PIN to an easily guessable PIN;
    - Sending users text messages to confirm that instructions have been received to change a PIN;
    - Suspending mailboxes when PINs have been entered incorrectly; and
    - Preventing more than one handset from accessing a mailbox at the same time.

What advice do we give to our customers on how they may protect themselves?

11. We have stringent security controls which deter unauthorised access to customer accounts.

12. Our customer services representatives are trained to provide advice to callers who seek assistance in protecting the confidentiality of their accounts, if they feel that their public profile is such that additional security measures are appropriate.

13. Some users are also provided with a tutorial when they first call their mailbox, which includes advice on changing their PIN.

Do we pass on to our customers any suspicions that their mobile communications have been intercepted and misused?

14. 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.

15. We do not consider it strange for callers to access their mailboxes from a phone other than the one they normally use, as this is a feature of the service we provide.

16. If a mailbox is suspended because a caller has entered their PIN incorrectly, they need to contact our customer contact centres to reset the PIN. This provides us with an opportunity to properly authenticate the caller before allowing them to access the mailbox. The protective measures we have in place to prevent voicemail abuse do not include automatic alarms to a central control centre to warn, say, our fraud teams, that particular accounts have been suspended.

17. Even if an allegation were to be made that a caller had inappropriately accessed a mailbox by using the correct PIN number, our transmission records only provide an investigator with limited information about what the caller had done once they had accessed the mailbox. Our records would indicate how long the call had lasted, but they do not log whether the caller had listened to, created or deleted particular messages.

18. We are happy to provide additional information, if this would be of assistance to the Committee.

October 2010

Memorandum submitted by Vodaphone

Thank you for inviting Vodafone Limited to contribute to your inquiry into the unauthorised tapping or hacking of mobile communications.

I understand your evidence session specifically relates to the voicemail incident which took place in 2006.

To provide you with the background, it is believed that journalists contacted customer services with details which enabled them to pass our security checks. They then selected their own PIN which they subsequently used to remotely access other people's voicemail.

This incident does not conform to the legal definition of tapping which is defined within RIPA as

"the use of devices to intercept a telephone transmission for the purposes of electronic eavesdropping".

These devices or 'bugs' as they are commonly known, may be planted legally or illegally and would not require somebody to use a PIN code set against a customer's voicemail in order to listen to the message.

What happened here was an example of social engineering, or in other words, an illegal act by persons who falsely represented themselves as Vodafone customers in order to access the accounts and change PIN numbers.

This offence may be considered to fall within the definition of unauthorised hacking where there is an unauthorised attempt to bypass the security mechanisms of the network. It may also constitute illegal intercept, where a third party is able to access the voice mailbox and listen to the transmitted message before the intended recipient has done so. It would be for a police investigation to determine the nature of the offence that has been committed.

Throughout this document, we have therefore not addressed the issue of unauthorised tapping. We refer throughout this note to the incident being an example of social engineering, illegal interception or unauthorised hacking. We would also like the Committee to note that this document neither contains any admission in any way of any liability on our part nor any legal analysis or statement which should be regarded as legally binding on us.

Background

As you know, Vodafone takes its responsibility to protect customers' privacy very seriously. We review and update our security procedures on a regular basis and we co-operate fully with police when crime is committed.

Your letter highlights a number of points that you would like us to cover:

i. How widespread the problem is
ii. What our company is doing to monitor and prevent unauthorised hacking or unlawful interception
iii. What advice we give to customers to help them protect themselves
iv. Whether our company alerts its customers to suspicions that their mobile communications may have been intercepted or misused.

i) How widespread the problem is.

We believe that a small minority of customers were targeted by unscrupulous individuals. At the time of the investigation we provided all evidence to the police.

It is not, however, possible for us to provide a precise picture of how widespread the problem was at that time. This is because an analysis of our records may show that a number has been accessed but we cannot state with certainty that the access was an unauthorised hacking attempt. As an example, a customer might access their account from a home landline, mistype their PIN or accidentally press keys with their head or ear. All of these might appear to be an unauthorised hacking or illegal intercept attempt when in actual fact the unsuccessful access attempt has been carried out by the contract holder. Most commonly, a customer may forget their voicemail PIN code and make several attempts to guess the PIN code in order to access their voicemail remotely. Again, this failed attempt to access voicemail by the account holder would be indistinguishable on our systems from an unlawful attempt made by a third party.

This problem occurred in the past and it is no longer a current problem. The changes Vodafone has instituted mean that this type of activity is no longer possible.

ii) What our company is doing to monitor and prevent unauthorised hacking or illegal intercept.

Following the 2006 incident, Vodafone carried out a root and branch review of its processes to make it harder for these individuals to target our customers. There was no evidence of any collusion whatsoever with Vodafone staff but we were determined to address any security issues and make the system as robust as possible.

As a result of this review, we implemented changes to our internal processes and voicemail systems in order to prevent this type of abuse from occurring in the future.

The changes included:

1) Ensuring the PIN is not accessible by front-line customer service staff: In the past, a front line customer agent could access a PIN to reset it. Our front line customer agents no longer have this access. Instead, the customer's voicemail PIN is reset and a new (randomly generated) PIN is generated. This prevents "social engineering" by a fraudster or someone impersonating a customer, passing the relevant verification checks and gaining unauthorised access.

2) Sending an SMS alert to the user: If an unsuccessful attempt is made, an SMS is sent to the handset to alert the user. If a customer then alerts us to the fact they have not caused the failed access, we can look at the logs over a two week period to see what numbers have dialled in and what digits were pressed. Outside that two week period we can check to see what call caused the text message failure. If it does appear to be a malicious attempt then we can provide evidence to law enforcement if required.

3) Conducting regular security audits across all business: We take special care to ensure our security processes are not breached. We do so by ensuring our employees have the training they need to adhere to the security policies and we conduct regular security audits to prevent accidental or deliberate breaches.

iii) What advice we give to customers to help them protect themselves

Vodafone has several pages on our website at www.vodafone.co.uk which are dedicated to voicemail PIN codes and security.

In terms of voicemail security and set-up, Vodafone customers have a choice when setting up their voicemail about how to protect it. They can choose from two levels of security: standard security (which is the default security level) or complete security.

Complete security requires the customer to enter their chosen PIN every time they access their voicemail, including from their mobile handset. Standard security does not require the PIN to be entered when accessing voicemail from the mobile handset but will require the PIN to be entered when trying to access voicemail from another phone or when abroad.

Vodafone's default security settings mean that a PIN is required when accessing voicemail remotely (that is, from a phone other than the relevant mobile handset).

As stated above, in order to prevent social engineering, our front line customer service staff cannot access a customer PIN. Therefore customers cannot call our customer services team to be reminded of their PIN should they have forgotten it. In this circumstance, the

customer's voicemail PIN is reset and a new randomly generated PIN code is sent to the customer's handset via SMS.

iv) Does Vodafone alert customers to suspicions that their mobile communications may have been intercepted or misused?

As stated earlier, it is not always possible to ascertain whether an account holder has been subject to an authorised hacking attempt. At the time of the 2006 incident, Vodafone issued general security advice to a number of customers believed to be in high risk groups. This was in line with the guidance we received from law enforcement agencies about the level of information we could release to customers.

If a customer contacts us with a concern about a failed access attempt which they do not believe they have caused themselves, we will investigate to ascertain whether it was an unauthorised hacking or illegal intercept attempt. In compliance with relevant data protection requirements, Vodafone would provide this data direct to law enforcement agencies on receipt of a RIPA request, on receipt of an authorised solicitor's request or following an appropriate Court Order.

November 2010

Memorandum submitted by Ofcom

As the Committee will be aware, the interception of telecommunications is governed by the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA sets out that, aside from certain exceptions, warrants are required before interception can be legally undertaken. The Act also gives powers to the Secretary of State to issue orders which impose obligations on providers of telecoms services to ensure they are able to provide assistance in relation to complying with such interception warrants.

The Act creates the role of Interception of Communications Commissioner, to oversee much of its operation. Ofcom has no role in the issuing of, or complying with, these RIPA warrants or orders or indeed any other aspect of the operation of Chapter 1 (Interception). Therefore, beyond noting the general requirements placed on all communications providers by RIPA, Ofcom has no knowledge of the obligations on mobile network operators (MNOs) from any orders which may be in place.

In terms of the general obligations placed on providers of telecoms services by RIPA, these include:

> Where a copy of an interception warrant has been served... on...a person who provides a public telecommunications service... it shall... be the duty of that person to take all such steps for giving effect to the warrant as are notified to him by or on behalf of the person to whom the warrant is addressed;

and:

> The Secretary of State may by order provide for the imposition by him on persons who...are providing ...public telecommunications services... of such obligations as it appears to him reasonable to impose for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with...

> It shall be the duty of a person to whom a notice is given... to comply with the notice; and that duty shall be enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief;

and:

> It shall be the duty of the Secretary of State to ensure that such arrangements are in force as are necessary for securing that a person who provides... a telecommunications service, receives such contribution as is... a fair contribution towards the costs incurred, or likely to be incurred, by that person in consequence of...the issue of interception warrants relating to communications transmitted by means of a telecommunication system used for the purposes of that service.

Data Retention

Another relevant piece of legislation in this context is the Data Retention (EC Directive) Regulations 2007. These Regulations require all public communications providers (which would include the MNOs) to retain data that is generated or processed while providing a communications service, for a period of 12 months. In the language of RIPA, the data referred by these Regulations is "communications data" which includes data associated with a communication, but is not the content of the communication itself.

The Regulations appoint the Information Commissioner as the Supervisory Authority. As with RIPA, Ofcom has no role in the relation to the Regulations, and therefore has no additional background on their operation beyond that which can be found in the text of the Regulations themselves. This is summarised below.

In the context of mobile telephony, the following data is specified by the Regulations for retention:

- the telephone number from which the telephone call was made and the name and address of the subscriber and registered user of that telephone;
- the telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred, and the name and address of the subscriber and registered user of such telephone;
- the date and time of the start and end of the call;
- the telephone service used;
- the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the telephone from which a telephone call is made;
- the IMSI and the IMEI of the telephone dialled;
- in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated;
- the cell ID at the start of the communication;
- data identifying the geographic location of cells by reference to their cell ID.

The Regulations specify a number of data security principles that should be adhered to in relation to the retained data:

- the retained data shall be of the same quality and subject to the same security and protection as those data on the public electronic communications network;

- the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
- the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and
- in the case of data retained solely in accordance with regulation 4(1), the data shall be destroyed by the public communications provider at the end of the period of retention.

November 2010

Memorandum submitted by Max Mosley

Until November 2009, I was president of the Federation Internationale de ('Automobile. In 2008 the News of the World (NOTW) published a story about my private life. I sued for Breach of privacy and was awarded damages and costs.

In pursuing its story about me, the NOTW engaged in criminal conduct. Such conduct is endemic at the NOTW and its parent company, News Group. The Metropolitan Police are aware of this. Yet only one NOTW employee has been prosecuted and no proper investigation of criminal conduct by these organisations has taken place.

NEWS INTERNATIONAL

1. Blackmail

The NOTW published its first story about me on 30 March 2008. It wanted a follow-up. To this end, its chief reporter, Neville Thurlbeck, set out to blackmail two of the women involved. He sent them emails threatening to publish their pictures in the next edition of his newspaper if they did not give him the story he wanted. This is described in detail in the judgement of Mr Justice Eady (Ref. [2008] EWHC 1777 (QB)), starting at paragraph 79.

As Mr Justice Eady pointed out "it is elementary that blackmail can be committed by the threat to do something which would not, in itself, be unlawful" (paragraph 87).

During the trial, Mr Justice Eady asked the editor of the NOTW, Mr Myler, if he had raised this matter with Mr Thurlbeck. The judge described his reply as "a non-answer, from which it would appear that Mr Myler did not consider there was anything objectionable about Mr Thurlbeck's approach to the two women as he did not query it at any stage. This discloses a remarkable state of affairs." (paragraph 86).

Since then, despite it being clear that Mr Thurlbeck had committed a serious criminal offence, no disciplinary proceedings of any kind have been taken by News Group or the NOTW. Nor have the Metropolitan Police taken action. Mr Thurlbeck is still chief reporter of the NOTW.

This reveals a culture of criminality at News Group. No law-abiding organisation would simply ignore serious criminal conduct by one of its senior employees.

2. Phone Hacking

The NOTW used a private detective, Glenn Mulcaire, to hack illegally into the voicemail messages of people of interest to the newspaper. Mulcaire and a NOTW reporter, Clive Goodman (the only NOTW employee prosecuted in recent years), were convicted of

unlawful interception of communications and conspiracy. Both went to prison in January 2007.

In 2009, Colin Myler, Tom Crone and Andy Coulson, respectively current editor, legal manager and editor in 2006 of the NOTW, told the Culture, Media and Sport Select Committee that no one but Goodman was involved in phone hacking: (Second Report of Session 2009-10, Volume II. Evidence at Q1331, Q1342 and Q1550).

It is my understanding that there is a mass of evidence in the hands of the Metropolitan Police which proves this claim is false.

News Group have paid very large sums of money to settle actions when faced with court orders for disclosure relating to phone hacking. In each case the sum paid was far higher than any damages the complainant could have hoped to secure in court.

The reason for this generosity is that News Group know disclosure would reveal the evidence currently held by the police and show that other reporters and senior management from News Group and NOTW were fully involved in phone hacking.

It is striking and worrying that the material which has been suppressed by News Group in these civil actions by means of very large payments, has been in the possession of the Metropolitan Police since August 2006. And yet, as they acknowledged in correspondence with the Select Committee (above Report at EV 356 - EV 358), they failed to investigate this material at the time of their original enquiry. They continue to refuse to investigate it now, with the result that they have taken no action to deal with the criminal behaviour disclosed by that material.

The newspaper also told the Select Committee (Myler at Q1331) that it had stopped the practice of phone hacking after the Goodman case. This is untrue. In April 2010, another NOTW reporter, Dan Evans was caught hacking into voicemails from his phone in the NOTW offices. He has been suspended from his work ever since (following a claim against him and the newspaper), yet the Metropolitan Police have taken no action.News Group's business methods include criminal offences. It has shown contempt for the law and, by virtue of its employees' false evidence to a Parliamentary Select Committee, contempt for Parliament itself. Yet the Metropolitan Police have not acted and continue to treat it like a normal commercial company.

3. Other anti-social conduct by News International

Apart from clear criminality, News Group and the NOTW resort to intimidation whenever their interests are threatened. Much of this may involve blackmail. There have been numerous well-documented threats to members of Parliament, including government ministers. There have been frequent allegations that actors, business people and journalists have been threatened, sometimes by very senior News Group employees, to prevent them suing or giving evidence.

Conduct of this kind is, of course, potentially criminal. Again, the Metropolitan Police have not investigated these threats even though some of them have been widely reported in the news media.

The Metropolitan Police will have been aware that a private detective, Jonathan Rees, was re-hired by NOTW in 2005 after serving seven years for planting cocaine in the car of a divorced woman to help her former husband gain custody of their children. The NOTW also used John Ross, a former detective sergeant who was sacked as a corrupt officer.

THE METROPOLITAN POLICE

When they arrested Mulcaire, the police searched his office and seized his papers. His papers will have included in each case details of the NOTW's target as well as the identity of the journalist giving the instruction. It was evident at Mulcaire's trial that journalists other than Goodman were involved.

Even a cursory examination of these papers will have identified a number of NOTW journalists who had commissioned potentially illegal investigations by Mulcaire. Evidence emerging in litigation involving News Group suggests that at least two senior members of the NOTW staff were involved, namely: the NOTW news editor Ian Edmondson and NOTW chief reporter Neville Thurlbeck.

Although the police visited the NOTW offices and searched Goodman's desk and computer, taking away material, they did not search desks or computers used by Edmondson or Thurlbeck, nor those of any NOTW journalist except Goodman. No attempt was made to question any NOTW journalist except Goodman.

The person in charge of the police investigation in 2006 was Assistant Commissioner Andy Hayman. Mr Hayman left the police in December 2007 and has been employed to write for News Group publications thereafter.

An explanation for Mr Hayman's failure to question Edmondson and Thurlbeck was offered by his successor, Assistant Commissioner John Yates, in evidence to the Select Committee on 2 September 2009 (Report at Q1890).

According to Mr Yates, Mr Hayman decided a polite enquiry to the NOTW's solicitors was preferable to questioning Edmondson and Thurlbeck or searching their computers and desks (see also, eg, Q1938 and Q1960). Unsurprisingly, given the nature of the organisation he was dealing with, Mr Hayman's letter seeking information drew a "robust" refusal (Report at EV 366/377).

What is extraordinary about the conduct of the police, indeed beggars belief, is that it must have been clear to them on the face of the papers seized from Mulcaire, that instructions to hack phones came from journalists other than Goodman including the NOTW news editor, Ian Edmondson, and the NOTW chief reporter, Neville Thurlbeck.

Edmondson and Thurlbeck were, at the very least, participants in the *very* conspiracy for which Goodman and Mulcaire were sent to prison. Yet neither was questioned or arrested, nor were their desks or computers searched.

Here was criminality so serious that Goodman, a first offender with no criminal record, went to prison. Yet the police, despite their direct knowledge from the evidence in their possession, made no attempt to investigate the senior NOTW journalists who were apparently guilty of the same crimes as Goodman.

What makes the conduct of the police even more extraordinary is that among the names of the NOTW's targets were not just so-called celebrities and sports personalities, but senior politicians including cabinet ministers. Worse, the great majority of those targeted by the NOTW were not informed by the police that their phones may have been hacked into and their security compromised.

The Metropolitan Police not only failed to follow the evidence, they suppressed it and continue to do so. It is deeply disquieting that they should pull back from investigating a powerful media group despite clear evidence of systemic criminal conduct. It is

unclear whether this failure to act is from fear of News Group's reaction of for other reasons

In order to restore public confidence, an in-depth and transparent investigation is now essential. Independent lawyers should be tasked with examining all the Mulcaire papers held by the Metropolitan Police and listing the News Group and NOTW employees who instructed Mulcaire together with the frequency and nature of their instructions. If necessary, an investigation by an independent police force could then follow.

SUMMARY

On the face of it, there appears to be endemic criminality on a significant scale within the News Group organisation and a failure by the Metropolitan Police to investigate, despite having extensive evidence of wrongdoing in their possession. It is now probable that the entire question will come before the High Court in proceedings for judicial review. Nevertheless, I submit that what has happened is so disquieting that a full independent enquiry has become essential.

December 2010