Haydon Dean - SOHQ

From: Williams Philip N - SCD11
Sent: 20 July 2009 18:13
To: Surtees Keith - SCD11; Haydon Dean - SOHQ; Saleh Naz - DLS
Subject: CPS - Investigation and Prosecution Challenges

Attachments: CPS - Investigation and Prosecution Challenges.doc

CPS - Investigation and Prosec...

Dear All

Following today's DPP meeting the attached is the document I sent to Simon Clements, CPS outlining the challenges, including technical, faced by the investigation and my observations on what the challenges would have been in relation to the Neville e-mail. What was true then in terms of challenges would be equally true today.

Many thanks

Philip

Challenges faced in the investigation and subsequent prosecution

1. Introduction

This briefing is intended to provide the CPS with an overview of some of the challenges posed by this investigation back in 2006, particularly in terms of bringing a case of interception of voicemail to trial. Those challenges would largely apply today subject to the fact that as a consequence of this case, the airtime providers have since introduced a range of measures to prevent a reoccurrence.

At the time, the investigation and prosecution strategy came to centre on the following key factors: -

> *1. S1 RIPA* - we would seek to prosecute any offenders under S1 RIPA for interception. It was ***the*** substantive offence out of what we were looking at. In theory the simplest/clearest to present in court and had the greatest sentencing power.
>
> *2. Technical* - In order to secure the willingness of victims to come forward as witnesses this case would be proved by technical means wherever possible as opposed to the playing of audio tapes/ making public of who left what message on a voicemail for who. This was the only way that we could secure the trust and cooperation of the primary victims with whom there was best evidence. This courtesy was extended to any other potential victims to protect as far as possible their privacy and treat them all fairly and equally.
>
> *3. Case Law* - there was virtually no case law in what we were setting out to achieve and therefore this would be groundbreaking. We were also seeking to push the boundaries of what interception was in an untested highly controversial area. This is no truer when it comes to the media/press and the never ending arguments around the balance between rights to 'intrude' on people's private lives in the public interest. It was anticipated that this would be groundbreaking and that unless there was overwhelming evidence it would be hotly contested by the media/press.

2. Challenges

The Law - S1 RIPA

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. Further the initial level of proof being worked upon was, a) to prove a mail message had been left, b) to prove that message had been accessed prior to it being opened by the intended recipient.

Mobile Phone Voicemail

In broad terms each mobile telephone is sold to customers with two unique telephone numbers. One is the number we all recognise and use to contact each other, the phone number. The second is created to access our voicemail messages attached to our telephones and is only used to remotely access our messages, so for instance we can access our own voice mail messages from a landline telephone by ringing this number. It is in effect what your telephone does automatically when you dial 121 on your handset. There is a slight variation with Orange who give customers a generic voicemail number into which you then input your individual phone number followed by Pin number. The only level of security after accessing this voicemail number is to have a Pin number which many customers simply leave at default or factory setting. For those who had customised their Pin, Mulcaire used a subterfuge with the respective airtime provider customer services to simply change it back to default and then access the messages.

Airtime Providers Support

The UK at the time had 5 main airtime providers, Vodafone, O2, Orange T Mobile and G3/Hutchinson. The former 3 were the main providers for the victims selected. All airtime providers were approached and were willing to assist, but on a fast degrading ability their engineering software was unable or did not exist to be able to provide a 'technical' picture of what was happening with voicemails being left and picked up on our victim's phones.

It is important to explain that each phone company uses its own software/data management systems to provide and monitor their service. In terms of prosecution these layers of engineering tools/software are not used for court purposes as in many case the integrity of what they show is not sufficiently accurate. Vodafone used engineering software called 'Vampire' data that showed with a higher degree of accuracy what was going on in terms of data entering and leaving mailboxes including timings. These could be matched to events/witness statements. During the early investigation there was also an additional proactive phase of the operation with regards to the Private Secretaries to try to overcome some of the inadequacies of the data systems by seeking to corroborate what our victims were experiencing matched against the data provided.

This had mixed results. In the case of Helen Asprey she had 'ported' her mobile number across a number of airtime providers including Vodafone, O2 and Orange which all added to the lack of confidence in terms of what could be proved in terms of her e-mail interception. In the end the only victim for which there was believed to be absolute proof was Jamie Lowther-Pinkerton (JLP). This evidence was based upon Vodafone 'Vampire' data and in particular it included a period when JLP was overseas which brought in another engineering tool called TAP Files (Transferred Account Procedure). By combining these two sets of data together with JLPs verbal recollection of what was happening to his voicemail it provided our best evidence of actual interception. This

evidence was presented by a mobile phone forensic engineer (expert witness) - Mr. David Bristowe.

All of the evidence for the other victims was built around the 'best fit' centered on the victim selection criteria thereby combining whatever we could show in terms of technical data with statements from the victims themselves providing it did not require them to reveal intimate details of actual conversations /other parties. Thus, based upon success with the JLP evidence, they all stood or fell together in terms of trying to represent the scale and breadth of what was happening.

None of the other airtime providers had engineering software/tools that matched this capability and Orange actually had to write their own software program to assist us and even then it could only cover a current three month period, all prior data having been destroyed. The victim Gordon Taylor used the Orange network.

Each of the Airtime providers took immediate steps to rectify the issues within their own organizations and thereafter a range of changes have occurred in the industry including enhanced customer information on how to protect their individual privacy to more robust customer service and preventative measures to prevent future interception for all customers.

Victims

As already highlighted a key factor in the investigation/prosecution strategy was to prove the case on technical data rather than risk the potential of discouraging victims, because of the sensitive nature of any conversations that may have been intercepted. This was and I would suggest remains a factor. Some of the potential victims did not wish to be part of a prosecution and it may still be that many would not want it to be known that they were even a person of interest for fear of what it might suggest about themselves.

An additional factor was that at first glance a victim was the recipient of the voicemail, but if we were to include any 'recordings' or accounts of who had left what message for whom that would thereby bring in third parties adding to the sensitivities and the need to be mindful of a much wider group of potential victims.

Covert/Overt

The initial enquiry was covert, firstly in order to establish what was going on and thereafter because it was recognised that the scale could be quite significant with the potential for damage to national security. It remained covert until August 2006 in order to try to establish the true scale without alerting potential suspects.

When it went overt on the 8th August 2006 it was recognised that although the full potential for this type of interception was not known, anyone who for whatever purpose had been utilising this method of listening to voicemails would now know that police

were investigating. Examples of how this affected the investigation and would potentially remain a challenge today are: -

- On the day of the arrests and searches News of the World (NOTW) actively engaged their lawyers to limit our ability to search during the actual searches and only cooperated as far as they had to thereafter.

- Although a Production Order was considered, advice resulted in us seeking access to material/information through cooperation with the NOTW legal department. Whereas NOTW solicitors were keen to point out that, *'Newsgroup Newspapers wishes fully to assist your investigation and does not require any formal Court order for the provision of any material. They are, however, entirely satisfied that the material to which you are entitled is limited.'* In relation to our enquiries about their internal telephone system, itemised telephone records and in particular details that might reveal who was called by whom before and after 'unlawful calls' they were quick to point out that *'it is highly likely that such information will amount to confidential journalist material.'* Then as now, these are reflective of just some of the challenges that any investigation would encounter when it comes to 'investigating' the media.

- Clive Goodman and Glen Mulcaire chose to make no comment to any questions posed throughout the investigation. In the case of the former, Clive Goodman was represented by NOTW legal team. It would not be unreasonable to believe that this would be the stance of anyone else who we sought to interview.

Searches and Material Found

The searches and seizure of material all took place on the 8th August 2006. In the case of Clive Goodman his home and office at NOTW was searched. The offices of 'Nine Consultancy' used by Glen Mulcaire and his home address of 108 Alberta Avenue, Cheam, and his parents address were also searched yielding a huge quantity of documents. Hundreds of handwritten sheets showed research into many people in the public eye. These included those linked to the Royal Household, Members of Parliament, military staff, sports stars, celebrities and journalists. There was also a quantity of electronic media recovered including recordings of some apparent voicemail conversations. It is reasonable to expect some of the material, although classed as personal data, was in their legitimate possession, due to their respective jobs. It is not necessarily correct to assume that their possession of all this material was for the purposes of interception alone and it is not known what their intentions was or how they intended to use it.

3. The 'Neville' e-mail

The above represents the backdrop of challenges faced during the investigation and subsequent prosecution. Applying them specifically to the e-mail allegedly sent by Ross Hindley on the 29th June 2009 I would make the following observations: -

- The e-mail from Ross Hindley dated 29th June 2005 was found as a paper copy at Mulcaire's home address in Alberta Avenue on the 8th August 2006. This document was then at least 14 months old and our case was focused on activity against potential victims in 2006.

- There is nothing on the document to suggest when the alleged conversations in the document may have occurred, but it would have been prior to the date of the e-mail.

- In relation to trying to secure telephone data to support any alleged interception we already knew from Orange (Gordon Taylor used Orange) that they could only provide current data which applied to a 3 month period in 2006. Therefore there would be no data for the period in June 2005 or before. Orange had to write specific software to be able to analyse and identify details of potential interceptions for the period in 2006. This would not be possible for 2005.

- The other companies held data historically for between 6 months and a maximum of 12 months. Therefore the same would apply to them if it became relevant in terms of trying to look back to June 2005 or earlier.

- There was nothing to say that Neville had actually seen the document. Even if the person 'Neville' had read the e-mail, that in itself is not an offence and therefore there was no evidence to link him to a conspiracy to intercept communications.

- There is no clear evidence of the identity of 'Neville' - it is supposition that it refers to Neville Thurbeck or indeed any other Neville within NOTW or elsewhere.

- Mulcaire's computers were seized and examined, nothing in relation to Neville or Neville Thurbeck was indicated.

- Given the robust stance of NOTW as soon as the matter became public it would not be unreasonable to believe that anyone questioned/interviewed in relation to the whole investigation would do anything other than exercise their right of offering 'no comment.' Both Mulcaire and Goodman exercised this right the latter being advised by the NOTW legal team.

- Under the criteria of not seeking to use anything that contained reported conversation (to preserve the sensitivities of victims/ third parties), the e-mail

would not have been chosen as part of the evidence put forward for Gordon Taylor in the prosecution case, but it was part of the sensitive unused material.

4. What did we achieve overall?

Against this backdrop I believe that we achieved a significant step forward in terms of potential intrusion on privacy in that: -

- **Case Law** - It has now been firmly established for the first time that this type of behaviour is unequivocally unacceptable. What is more, it is a criminal act and you will go to prison if you do it. I believe that is a powerful achievement, in what is often viewed as a murky and frequently contested arena.

- **Protection of the Public** - Through the close cooperation and involvement of the airtime providers this type of intrusion has been aired in public and they have brought in a range measures to prevent it in the future. The wider, greater need has thus been addressed in terms of personal intrusion and indeed the potential risk to national security.

Philip Williams
Detective Chief Superintendent
Monday 20th July 2009

NOTE

This document contains material that is sensitive to the airtime providers in terms of past potential vulnerabilities as well as methodology. Care should be taken in terms of exact detail that might be made public.