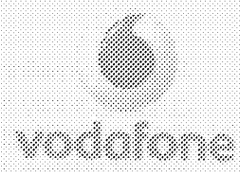

Khaleel Desai
Assistant Solicitor to the Inquiry
The Leveson Inquiry
c/o Royal Courts of Justice
Strand
London WC2A 2LL

By Email only: solicitorlevesoninquiry@tsol.gsi.gov.uk

12 October 2011

Dear Mr Desai

Re: Section 21 Notice

I write further to the request in your section 21 notice for an explanation of how a mobile phone can be hacked or voicemail accessed and the steps that can be taken to prevent this from happening. I set out below Vodafone UK's response to this request.

Phone Hacking

The term 'phone hacking' is usually taken to refer to the illegal interception of telephone calls, which may include voicemail messages. As the Chairman will be aware there is a comprehensive framework of legislation that deals with the unlawful interception of telecommunications. In particular, section 1 of the Regulation of Investigatory Powers Act 2000 (RIPA) makes it a criminal offence to intercept, without consent, any communication "in the course of transmission" on a public or private communications network (subject to specified exceptions when this is permissible for government agencies). Section 2(7) of RIPA defines "transmission" to include any communication which has been transmitted and stored for the intended recipient to have access to it, such as voicemail messages.

Vodafone is one of a number of mobile network operators in the UK who offer customers access to a public telecommunications system. In 2006 it began assisting the Metropolitan Police Service (MPS) with an investigation in to unlawful access to voicemail messages on public telecommunications systems. As far as I am aware, the MPS investigation and the matters now being examined by the Chairman relate only to access to customer voicemail messages and not, for instance, to the interception of live telephone calls.

Vodafone Limited
Legal & Government Affairs
Vodafone House, The Connection, Newbury, Berkshire RG14 2FN, England
T +44 (0)1635 33251 F +44 (0)1635 676197 www.vodafone.com

From information provided by the MPS, it is understood that the voicemails of a number of Vodafone customers may have been accessed illegally by criminals in possession of a customer's PIN. Importantly, the unauthorised access does not appear to have involved any breach of the Vodafone communication servers through the use of eavesdropping devices or other technology. I have therefore referred to the unauthorised accessing of voicemails as 'blagging' rather than 'hacking' as it appears to have involved some level of deceit in obtaining customer account information to gain access to voicemails.

Unauthorised Access of Voicemails

All voicemail messages are encrypted on the Vodafone voicemail platform and only decrypted at the point of delivery. At no point is it possible for voicemail messages to be reviewed by anyone (including Vodafone personnel) other than the person operating the customer's handset and/or in possession of the customer's voicemail PIN.

Access to voicemails is possible both from the customer's handset and 'remotely'. Remote access covers access using a telephone other than the customer's handset as well as access whilst roaming (whilst abroad). Since 2001, remote access to voicemails has only been possible with a personal four digit PIN. For the avoidance of doubt, default PINs are not used. Prior to 2006 it was possible for customers to call Customer Services and, providing they passed the caller verification process to confirm their identity, to ask the adviser to set a remote access PIN of their choice.

In 2006, Vodafone was notified by the MPS that certain unauthorised individuals may have accessed some Vodafone customer voicemail accounts unlawfully. It is understood that unauthorised access may have been gained by these individuals either guessing and then using the customer's remote access PIN or by procuring or re-setting the customer's remote access PIN to a number of their choice. These are matters still subject to the Operation Weeting police inquiry but I understand that it is possible that the 'blagger(s)' may have gained access by dishonestly pretending to customer services as an authorised person during the caller verification process and then procuring and/or re-setting the customer's remote access PIN.

Anyone in possession of a customer's remote access PIN and their mobile telephone number / unique voicemail number (the number used by Vodafone as the gateway to each customers' voicemail prior to 2006) would be in a position to deal with the customer's voicemails in exactly the same way as the customer themselves, that is to say they would be able to listen to and to delete any voicemail messages left on the customer's mobile phone and, in some instances, to learn of the telephone number used by the person leaving a given message.

Steps Taken to Improve Security

Vodafone has taken these concerns extremely seriously and ensures that all customers are provided with advice about voicemail security. Since 2006 Vodafone has also taken a number of technical steps to address the risk of unauthorised access to voicemails. These measures include:

- Ensuring that customers are no longer able to obtain, or re-set, a remote access PIN of their choice over the telephone to Customer Services.
- All customer voicemail PIN numbers are stored within a secure platform which has rules in place to check customer selected PIN numbers and which will reject weak PINs (e.g. 1234, 9999). PIN numbers

are stored in an encrypted format and cannot therefore be viewed by anybody, whether within Vodafone or externally.

- While customers may still request a PIN from Vodafone customer services, all such requests lead to an automatically generated random code being sent via text message to the customer's handset (not visible to customer services or indeed anyone else). Customers can also set their own PIN themselves through their voicemail menu using their own device and SIM. Customers can personalise their PIN through their voicemail menu.

- If a customer forgets their voicemail PIN then they can call Customer Services to request that it is re-set; however, as with requests for new PINs, requests for PIN re-sets lead to an automatically generated random code being sent via text message to the customer's handset. The customer service advisors cannot view or manually select customer PIN codes.

- If 3 unsuccessful attempts are made to access a customer voicemail account then a text message is automatically sent to the customer's handset advising them of the access failure and suggesting that they contact Customer Services if they are concerned that their voicemail account may be being targeted by an unauthorised third party.

- In addition to having a PIN to protect remote access (defined for customers as "standard" security), customers can also elect to put a PIN in place for all access to their voicemail messages, including from their own handset (enhanced, or "high" security).

- Customers are provided with information about voicemail security through the New User Tutorial (which all new voicemail customers are taken through automatically on the first three times that they dial into their voicemail) as well as through Vodafone's website (vodafone.co.uk). In particular, Vodafone encourages its customers to select the "complete security" option if they want all voicemail access to be protected by their PIN, to avoid selecting remote access PINs that could be easily guessed (e.g. customer date of birth, house number and any part of their phone number) and to change their PIN regularly. As before, if a customer chooses not to set a PIN, they will not have remote access to their voicemails. Customers are also advised to apply password/PIN protection to the handset itself (where available) and to keep handsets safe.

- If an employee believes suspicious activity is occurring on a customer's account Vodafone operates a "duty-to-report" policy so that employees can alert management or an anonymous whistle blowing hotline about those concerns.

Conclusion

Vodafone has made, and continues to make, strenuous efforts to increase the security of mobile communications and voicemail in particular. The need for constant vigilance against such threats is widely understood across all mobile network operators. There are no cast iron guarantees that it will be possible completely to eliminate the threat of blagging and unauthorised access of voicemails by criminals. However, Vodafone is committed to working with the other mobile network operators to ensure that systems are as secure as possible whilst ensuring that security features remain customer friendly and easy to use, thereby ensuring a high level of take up and use across Vodafone's customer base.

Error! Reference source not found.

3

I hope this information assists the Chairman. I would be grateful if you could notify me in advance about how you intend to use the detail provided. In particular, it would be helpful if you would explain whether and, if so how, it will be disclosed to Core Participants and/or the wider public.

Yours sincerely

Sarah Spooner
Lead Counsel
Legal and Government Affairs

Error! Reference source not found.

4