Leveson Inquiry www.levesoninquiry.org.uk

Disclosable Summary of briefing on Techniques of Access to Personal Data given by Charles Brookson on 19 September 2011

Mr Charles Brookson, of Zeata Security, provided a briefing to the Inquiry on 19 September on techniques of access to personal data.

The briefing was attended by Lord Justice Leveson, Lord Currie, David Bell, Elinor Goodman, George Jones, Shami Chakrabati and Sir Paul Scott-Lee. In addition, Counsel to the Inquiry and the Inquiry Secretary were present, along with other members of the Inquiry Secretariat and Inquiry legal team.

Lord Justice Leveson began by making an order under s.19 of the Inquiries Act 2005 restricting public access to this session on the ground that such restriction was in the public interest. This disclosable summary of this teach-in, covers those matters which may properly enter the public domain.

Mr Brookson began by referring to the various statutes that place limits on behaviour in relation to electronic communications and telecommunication networks. Specifically he reflected on provisions in the Regulation of Investigatory Powers Act 2000, the Telecommunications (Fraud) Act 1997, the Computer Misuse Act 1990, the Wireless Telegraphy Act 1949 and the Communications Act 2003.

Mr Brookson spoke about the many and varied ways of accessing e-mail without authorisation, including well known ones such as guessing passwords, malware – viruses or Trojans that can be planted on equipment by opening an e-mail, opening an attachment or visiting a website and then provide access to details of the e-mail account, and what he termed 'social engineering' – acquiring information from third parties by deceit, persuasion or bribery that would allow access to an e-mail account. He also spoke about more sophisticated variations on these techniques, how they might be used and how easy it was to adopt them.

He then moved on to issues around mobile telephone security. He said that the basic and well publicised method of hacking by simply dialling into someone's voicemail account was still technically possible. It was important that mobile phone companies should allow remote access to voicemail because it was a necessary part of retrieving messages from many foreign countries. Users could make that remote access more secure by changing their pincodes. Mr Brookson felt that the phone companies could do more to educate and encourage their subscribers to take security seriously on their phones and their voicemail. However, even where pincodes had been changed from the default it was still possible to gain access using social engineering techniques as described above.

Mr Brookson spoke about other means of obtaining personal data from mobile phones. He noted that data travels across different parts of a network to reach its destination and could in theory be intercepted at a number of different points and that different approaches could be used to intercept data at different stages on its journey. He said that security on 3G was significantly stronger than security on GSM and noted that some mobile phones will allow the user to only use 3G. However, this would be a trade-off between security and coverage since it is not always possible to access a 3G network.

He briefly discussed the risks of a sim card being cloned. He said this was something that was no longer possible with phones sold in the UK but could still be a risk with phones bought abroad if they were using an old standard.

Mr Brookson said that it is technically possible to locate and listen into a mobile phone call using equipment that is commercially available – a technique that was publicly demonstrated in December 2010, but that this is not a risk for 3G and is not currently a technique in widespread use.

He described other techniques for intercepting a call between the base station and the phone - the 'man in the middle' attack – and explained that this had become easier and cheaper to do in recent years. Again, this is not a risk for 3G.

Mr Brookson re-emphasised that the companies providing mobile services legitimately have access to substantial data about the phone user, in particular location data and data about calls they have made, voice mail etc. All this data is potentially susceptible to the social engineering techniques described earlier.

Mr Brookson finished by talking about the potential for unauthorised data access arising from mobile device issues. Many mobile devices now have a variety of ways to access data and these can provide information to third parties. If Bluetooth is switched on, for example, it will provide location information to third parties. Data stored on mobile devices can be accessed by malware (viruses, trojans etc) or obtained by some applications. Data can often be obtained from lost, stolen or sold mobiles, even when they have theoretically been 'wiped'.

It is possible to forge calling line identity to spoof a target's phone and get access to data or make false calls or send false text messages. As with fixed line access there are dangers from malware which can be planted on a mobile phone either via physical access or via an e-mail, attachment or webbrowser. Mr Brookson described software that is available on the internet that claims to be able to give access to all a mobile phone's data including recordings of calls.

It was noted that possession of the equipment or software needed to access computer or phone data in these ways was not illegal, but that the use of it to do so would breach the Data Protection Act and, depending on the specific technique

deployed, might breach one of the statutes listed above governing electronic communications and telecommunications.

This note intentionally does not cover the detail of any of the data access techniques referred to, nor does it cover all the techniques that were discussed on 19th September, but it does give a picture of the broad ground covered in the briefing.