CASE NOTE: SINGAPORE

CASE CITATION:
Public Prosecutor v Neo Khoon Sing [2008] SGDC 225

NAME AND LEVEL OF COURT:
District Court

DATE OF DECISION:
18 January 2008

MEMBER OF THE COURT:
District Judge Bala Reddy

Digital evidence; the standard of proof for circumstantial evidence; it should lead one to 'the irresistible inference and conclusion' that the offence was committed by the accused

Brief facts

The accused worked at an independent office at the National Environment Agency North East Regional Office (NEA NERO). He was co-leader of a sub-committee given the task of organising a two day event during NEA's 'Clean & Green Week 2005' (CGW 2005). On 18 October 2005 two false terrorist attack warning messages (alarming messages) were sent through the web sites of the Ministry of Home Affairs, the first of which read 'Rumours of possible suicide bomb in Bedok area in 2 to 3 weeks time' and the second of which read 'a possible bomb attack in Singapore in an event with water activities involving head of state, ministers etc. Within a month'. The third alarming message was sent through the web site of the Prime Minister's Office (PMO) on 19 October 2005, and read:

> 'I would like to inform you of a plot to conduct suicide bomb attack against PM, Ministers and MPs in a major event in Bedok Reservoir area in the coming weeks. The group mainly locals carrying out this attack are trained by an unnamed Thai Muslim fundamentalist group infamous for attacks against government soldiers in Thailand. The group has managed to infiltrate the National Environment Agency top rank management through a converted Thai Muslim who underwent Jihad training in Thailand early this year. The attack is likely to be carried out either by vessels loaded with explosives running into the VIP tent at high speed or by bombs concealed in drums, etc, used by performing groups. The attack is at the final phase and all equipment are ready for deployment. Please respond quickly'.

The alarming messages were communicated to the respective recipients via the feedback function in web sites, not by e-mail. Police investigations revealed that the alarming messages had emanated from NEA's computer network. In particular, they had been sent from the desktop computer located in the office (office computer) in which the accused worked, and which had been allocated for use by the accused.

The charges

The accused was served with three charges under Regulation 8(1) of the United Nations (Anti-Terrorism Measures) Regulations, which are read with Section 5(1) of the United Nations Act (Cap. 339) for sending false terrorist attack warning messages.

Defence raised by the accused

The accused claimed the defence of alibi, and also claimed that the e-mails were sent by an impostor who had access to his office. He called a digital evidence specialist to support his theory.

Defence of alibi

The accused claimed that on 18 and 19 October, on account that he had been afflicted with diarrhoea, and had gone home a number of times without informing anyone at NEA NERO. The accused called his father and wife as witness to corroborate his movement on the dates in question.

Prosecution's rebuttal of alibi defence

The prosecution's case was that because the messages in question were traced to the office computer, he was the obvious culprit. If a finding of fact is made that the accused sent work related e-mails during the same period of time that the messages were uploaded on to the web sites, then he must have been in his office at times closely proximate to activities relating to the sending of three alarming messages.

The digital evidence demonstrated that 29 minutes

after the first alarming message was sent, the office computer was used to log on to the accused's account through Lotus Notes. An e-mail was sent at 3:23 pm on 18 October 2005, and immediately afterwards the office computer was used to surf the Ministry of Home Affairs web site leading up to sending of the second alarming message. Thereafter, after a gap of 24 minutes, the office computer was used to log on to accused's account through Lotus Notes.

An e-mail was sent at 9:16 am on 19 October 2005. Shortly thereafter, at 9:27 am, the computer was used to search information at an on-line government directory for the address of the recipient of the third alarming message. At 9:29 am a work related e-mail was sent, and around at the same time a file 'PMO.doc' was created on the thumb drive (other names for thumb drives include: flash drives, jump drives, pen drives, key drives, and USB drives) of the accused, containing the e-mail address for the PMO.

The timings of sending of the e-mails and logging into the accused's account contradicted the accused's claim that he was not in his office at the time the alarming messages were sent.

The impostor theory

The accused claimed that some 'impostor' had entered his office and sent the three alarming messages. He also asserted that the six e-mails, which were relied on by the prosecution as corroborating evidence, had not been sent from his office computer. The accused claimed that his Windows password was his previous car license plate number, while his Lotus Notes password was his National Registration Identity Card (NRIC) number and had remained unchanged for past 10 years. He also claimed that he had recorded these two passwords, together with other password for the computer applications, on two pieces of paper and kept them in plain view on his desk.

Prosecution's case relating to the impostor theory

The accused acknowledged during the cross examination that it would be difficult for any impostor to enter his office, without a high risk of detection, and was unable to produce evidence that an unauthorised person had gained unauthorised access to his office in order to send three e-mails in question.

Initially, the accused admitted that he did not share his thumb drive with anyone. A number of files were recovered on the accused's thumb drive: 'PMO2.doc', '_WRL002.tmp' and 'PMO.doc', which were clearly related to third alarming message, and implicated the accused in the sending of the third alarming message. If the accused was not engaged in his usual routine on 18 and 19 October 2005, then it would have been next to impossible for any impostor to have sent those e-mails and messages, because an impostor would not have been able to predict his movements on the days in question.

The defence digital evidence specialist

With regard to the e-mails produced by the prosecution as corroborating evidence, the digital evidence specialist for the defence confirmed and agreed that there was no conclusive evidence to show that the e-mails had been sent from the office computer, but is was a possibility that the e-mails had been sent from the office computer. The digital evidence specialist stated that it was very likely that files attached to two e-mails had been opened on the office computer, and at least one attachment had been saved onto the hard disk of the office computer. The accused testified that he did no such thing. He claimed that he was on a field inspection at the material time but he was unable to substantiate this assertion.

The digital evidence specialist conceded that a hyperlink ('pmo_hq@pmo.gov.sg'), found in the file PMO.doc, could have been copied from a government directory web site. He did not dispute, however, that the office computer had been used to obtain access to the Public Service Directory Interactive Website at about 9.27 am (two minutes before the alarming message was sent) on 19 October 2005.

The text of the third alarming message was found in the thumb drive. The digital evidence specialist testified that his examination of the various links and temporary files that were relevant, revealed that it was possible that the file PMO2.doc had been created on another computer, saved on the thumb drive, and subsequently transferred on to the office computer. However, he conceded that it was also possible that the file was created on the office computer and subsequently saved on to the thumb drive.

Held

The prosecution relied on circumstantial evidence and the evidence in the statements of the accused to

establish its case. Bala Reddy J quoted a decision of the Court of Appeal respecting the test for the use of circumstantial evidence, at 66, and further commented in respect of the evidence in this case at 67:

> 66 The Court of Appeal followed the approach in Ang Sunny v PP,[1] and further
>
> stated:
>
> "The Sunny Ang test arose out of the following direction the trial judge gave to the jury in his summing-up at the close of the case:
>
> "Now, as I told you earlier on, one of the points about circumstantial evidence is its cumulative effect. Any one of these points taken alone might, you may think, be capable of explanation. The question for you is: where does the totality of them, the total effect of them, all lead you to? Adding them together, considering them, not merely each one in itself but altogether, does it or does it not lead you to the irresistible inference and conclusion that the accused committed this crime? Or is there some other reasonably possible explanation of those facts?"
>
> The prosecution case is that the effect of all this evidence drives you inevitably and inexorably to the one conclusion and one conclusion only: that it was the accused who intentionally caused the death of this young girl."
>
> 67 The thrust of the accused's defence is that he did not send the messages in question but an imposter did. It is not for the accused to prove that an imposter had in fact sent the messages. The burden to show that it was the accused who had sent the messages rests on the prosecution in order to establish the charges beyond reasonable doubt.

The defence was not able to create any reasonable doubt in this case. The judge found the imposter theory incredible as there was no one with the motive to frame the accused nor likely to have committed the acts undetected given the high risk. Further, the imposter must have had intimate knowledge of the accused's work process as well as of his involvement with the CGW 2005 to compose the alarming messages. In short, the learned judge found the evidence of the passwords being written down as a lame attempt to substantiate the 'imposter' theory.

The court concluded that the accused deliberately sent three alarming messages, peppered with alarming details of terror attack against the Prime Minister and other leaders at a public event. The accused was sentenced to 30 month's imprisonment.

Comments

This case serves as a reminder that digital evidence can serve to both support and challenge the theory of a case. The use of a defence that relies on a deficiency in digital evidence may be countered by further digital evidence, as well as other forms of evidence, such as documentary proof and oral testimony. Bare assertions rarely succeed, and the principles of relevancy and weight remain applicable. Another observation that may be made is that those responsible for collecting evidence continue to develop skills and methodologies in respect of digital evidence in order to counter every possible defence and issue that may be raised.

Bryan Tan is a member of the editorial board

[1] *[1966] 2 MLJ 195.*

