IN THE COUNTY COURT
AT MELBOURNE

(IN ITS CRIMINAL JURISDICTION)

THE QUEEN

and

ANDRE REMON DEDIO

SUMMARY OF FACTS

COMPUTER TERMINOLOGY: Some computer terms are defined at the rear of this document. They are denoted by an *

BACKGROUND

DEDIO and 2 other defendants. James Joseph CARTER and Julian Paul ASSANGE were charged as a result of an investigation by the Australian Federal Police Computer Crime Section. codenamed. Operation Weather.

The investigation commenced as a result of a number of complaints received by the AFP during 1990 and 1991 pertaining to illegal accessing of various computer sites. One of those sites was the Royal Melbourne Institute of Technology (RMIT). The AFP attempted to put line traces on RMIT computers in order to catch the intruders. The line traces met with an unusually high incidence of failures due to illegal manipulation of the telecommunications network by the hackers.

On 13 October 1990 successful line traces eventually identified the originating addresses of 2 of the RMIT computer hackers. Those addresses were 6-8 Gibbs Road, Montrose (telephone service 03 7281519) and 3 Bennett Street. Balwyn (telephone service 03 817 5611). They were the residences of Andre Remon DEDIO and James Joseph CARTER. respectively.

Intrusions into other sites, displaying a familiar pattern to what had occurred at the RMIT, led the AFP to believe that one group of hackers might be responsible for many of the intrusions being reported to them. Around October 1991 police attention was particularly drawn to the suspected activities of CARTER. and a telephone intercept device was placed

on his telephone service between 1 October 1991 - 29 October 1991. The monitoring of CARTER's line included both voice and computer transmissions.

After monitoring a number of CARTER's calls during the aforementioned period, it became clear that CARTER's two closest computer friends were DEDIO and ASSANGE, whom he communicated with regularly. The police were not afforded the opportunity of placing telephone intercept devices on DEDIO's and ASSANGE's telephone services because at the end of October 1991 Dedio apparently received a death threat from a fellow computer enthuisiast. He reported the incident to the Victoria Police, and in so doing, took the opportunity to advise them of his involvement in computer hacking. This in turn was reported to the AFP.

Warrants were executed on the homes of DEDIO, CARTER and ASSANGE on 29 October 1991. All three participated in lengthy interviews. Those interviews took place on the following dates - 29 October 1991 and 5 August 1992 (Dedio), 20 December 1991 and 12 February 1992 (Carter) and 20 February 1992 and 26 February 1992 (Assange).

After a lengthy investigation by the AFP DEDIO, CARTER and ASSANGE were charged in July 1994 with a variety of offences under the Crimes Act 1914.

DEDIO told police during his interviews that he commenced hacking* computers and phreaking* phonecalls in 1988 (folio 279). He used the call sign "Trax" or "Train Trax" (folio 22). His hacking occurred with the use of his personal computer, which was located at his home in Balwyn, together with a modem, which is a device which allows the computer to connect to external sites using the telephone lines. He told police that when he first got a computer of his own he logged into computer bulletin boards (BBS)*. One such bulletin board provided him with a file called "Aussie dialups*" plus encrypted password files and some cracked accounts. He also learned of the existence of an account called alt.security which he said was present on all university systems throughout the world. This account would often have information relating to security holes or bugs in computer systems. Assange also provided him with lists of cracked accounts. These sources of information gave him his first introduction to computer hacking. (folios 35 - 40; 75; 279)

He also told police that his hacking was motivated by the joy of breaching the security of a computer system and of gaining a reputation. He said that his activities were not malicious in nature (folio 32). DEDIO told police that he had never been paid to hack computers on behalf of other persons (folio 373). He also told police that he knew that he was doing the wrong thing by hacking (folio 76). He told police that CARTER and ASSANGE "were hackers on a major scale, on a huge scale. Something never achieved before" (folio 131) whereas he described himself to police as largely an interested observer in the hacking scene. He also told police that he believed ASSANGE and CARTER were getting in too deep and that they were driven to a point where they wanted to get caught. He said that he felt CARTER and ASSANGE were capable of anything and that they could cause a lot of damage (folio 132 - 133). Their activities had made him anxious about his involvement in computer hacking.

THE INDICTMENT

Count 1 Defraud the Commonwealth, s.29D Crimes Act 1914 - "phreaking"

DEDIO's technical ability was not so much his ability to gain unlawful access to computers, although he was clearly able to do this. Rather, it was his ability as a "phreaker" to penetrate systems and not be traced or charged for the calls he made. DEDIO was able to

successfully manipulate the telecommunications network using a technnique known as "tone dialling". "Tone dialling" is an instance of a larger phenomena known as "phreaking". With "tone dialling" special tones are sent down the telephone line by the "phreaker" to imitate those used by carriers to control the telecommunications network. These signalling tones are not normally used from customers' premises and are not available on a normal telephone keypad. The telephone network is not designed to receive these tones from a customer's equipment and may interpret them as internal signalling tones, which in the right circumstances can then result in the switching of the telephone call. When tone dialling is used by a phreaker the telecommunications carrier is generally defrauded.

DEDIO told police that he discovered how to phreak accidentally in 1988 when he was doing a scan. He heard heartbeats on his telephone line and didn't know what it meant. Some months later he was given a phreaking file by s47F alias Blind Greek God which Blind Greek God had found on a BBS called "Devils Playground". The file listed CCIT#5 signalling tones. DEDIO wrote a program to generate those tones. The next step, he said, was to scan an AXE telephone exchange for disconnected phone numbers (ie previously connected telephone numbers which had been disconnected). DEDIO told police that he knew when he had found a disconnected phone number because he'd hear a sound like 2 short heartbeats and then silence. He would then play the MFC signals (ie the computer generated tones) into the telephone line using an amplifier in the computer and this would cause him to drop into the disconnected telephone number (folios 45 - 52; 93 - 99; 370 - 371).

Phreaking is a useful tool in the armoury of a computer hacker. If the correct tones are played, as discussed above, the caller will be dropped into a telephone line. From there DEDIO could dial up a nominated computer. Not only would line traces on the victim site fail to trace any hacking back to its original source (eg see RMIT above), nobody, including DEDIO, would be charged for the telephone call made. Dedio admitted to police that he employed this technique in relation to his computer hacking. He also admitted to using it in relation to making telephone calls. He advised police that he would "phreak" international phonecalls to friends in Europe or Indonesia every 2 - 3 months and he would also phreak phonecalls overseas for his friends. He estimated that he had made around 20 such international phonecalls of approximately 10 - 15 minutes duration (folio 95). Phreaking has the effect of defrauding Telecom revenue. There is no way to estimate the amount that Telecom has been defrauded by DEDIO's phreaking activity. Phreaking calls to Victorian computer sites or interstate computer sites deprives Telecom of revenue to the equivelant of a local telephone call or STD call, depending on where the computer site is located . Dedio admitted to police that he had defrauded Telecom and that what he had done was wrong (folio 52).

Counts 2 - 4 - Obtaining access to data by means of a Commonwealth facility

(a) RMIT (counts 2 and 3)

DEDIO admitted to police that he had unlawfully accessed RMIT computers. The RMIT was, during 1990 - 1991, one of the most active computer hacking sites in Victoria with a large number of hackers active there at the relevant time.

The RMIT has many computer systems, each of them uniquely named. When individuals associated with RMIT wish to use the computers at RMIT, they are given an account on the relevant computer system(s). That account is password protected, which means that only the legitmate owner of that account, the systems administrator* or someone who has been given the account name and password information should have access to the account.

DEDIO is not and never has been a student at RMIT, nor did he have at the relevant time any other legitimate connection with that establishment. Accordingly, DEDIO should not have had access to any of the accounts on any of the RMIT computer systems.

DEDIO admitted to police that he was a regular hacker on RMIT computers, and that in the period of August 1991 - October 1991 he was accessing RMIT systems daily. To gain entry he would dial up the RMIT University Computer Annex using his computer and modem. He would then be given a prompt as to which RMIT computer he would like to connect to. He would then nominate a system which he already had an account for and type in the the name of that computer system. Once he had connected to that system he would be prompted for an account and password. He would then type in an account and password which were already in his possession. That would then given him access to the computer system.

Goanna and Yallara are both computers located at the RMIT. The Goanna machine was used by departmental staff and post graduate students conducting research, and was used for the preparation of coursework and research. It contained exam papers and from time to time exam results. The Yallara machine was primarily a student's machine, that is, a computer used by students in the preparation of their coursework.

DEDIO possessed numerous accounts on both the Yallara and Goanna machines and accessed those accounts (folio 330). They were student accounts. This would have given him access to any material stored on that computer by the respective account holders, including electronic mail. He told police that ASSANGE initially gave him an account on Yallara and that ultimately he had 3 or 4 accounts on Yallara (folio 299 - 300). Again, this would have given him access to any material in the account holder's account, including electronic mail.

DEDIO admitted to police that whilst he was on the Yallara system he had access to the password file for Yallara and that he had run a program called "Cops" over the password file in an effort to crack some of the password files. "Cops" is a security program which system administrators use to check for "dumb" passwords, ie passwords which are easily guessed using password cracking programs. There is no evidence to suggest that Dedio inserted "Cops" into the Yallara system, simply that he utilised it. He told police that his use of "Cops" allowed him to guess passwords pertaining to several student accounts on Yallara. He admitted utilising those student accounts (f. 307).

DEDIO also admitted to having accounts on Goanna. DEDIO copied the encrypted password file on Goanna and downloaded it to his own computer (copy appears at folios 571 - 578). He told police that he did not bother trying to crack the password file, as ASSANGE had already done that (f 363).

DEDIO told police that whilst he was on RMIT computers he ascertained which computers on the Internet were trusted hosts. He created a computer file, namely, Disk 4 side B - RMIT.TEL (folio 579 - 582), listing in numerical order, all of RMIT's trusted hosts. He admitted to police that he attempted to log into RMIT's hosts from the RMIT server, but with only limited success(folios 365 - 366).

The effect of hacking activitity on the RMIT was twofold. First, the integrity of RMIT systems was compromised during 1990 - 1991 by DEDIO, CARTER and ASSANGE, as well as other unknown hackers. In order to regain system integrity the RMIT Computer Centre on at least two occassions had to cancel all passwords on the system. This resulted in every RMIT computer user coming to the Computer Centre to be given a new password.

The RMIT has estimated that it spent between $10,000 - $20,000 in determining the nature of the attacks on its computers and determining the extent of any damage caused to its comp[illegible] A reparation order is not sought against DEDIO, CARTER or ASSANGE for this amount, given the fact that many other hackers were active at the site.

(b) Northern Telecom - Count 4

Northern Telcom Ltd is a Canadian company involved in the design and manufacture and maintenance of telecommunications equipment. including telephone exchange equipment for companies such as Telecom Australia. Northern Telecom and its subsiduaries operate approximately 15,000 separate computer systems internationally which are used in the ordinary course of its business. The computers are linked via a common communications system and this entire system is collectively known as CORWAN.

Between July 1991 - October 1991 Northern Telecom's computer systems were the target of computer hacking by a handful of hackers, including, DEDIO, CARTER and ASSANGE. The Crown contends that the evidence overwhelmingly suggests that ASSANGE was the primary hacker at Northern Telecom Ltd. It is alleged, interalia, that ASSANGE ran a TFTP program on a CORWAN systems known as NMELH1. That program was designed to grab password files from nominated sites and it is alleged that ASSANGE obtained over 1000 password files from Northern Telecom systems using this program. Over 100 gave him superuser access.

According to DEDIO, CARTER was the first of the 3 defendants to obtain access to Northern Telecom Ltd systems. According to DEDIO, CARTER gave an account of VO300 to ASSANGE. who then gave it to DEDIO (folio 48). This account belonged to a CORWAN system known as NMELH1. NMELH1 serves as a gateway to other CORWAN systems and it also serves as a temporary repository of "commercial in confidence" material which is being transferred from one computer to another. The account which DEDIO obtained from CARTER was an ordinary user's account, and it gave him access to commercial and personal information. DEDIO told police that he had limited involvement in the Northern Telecom systems, and that he accessed NMELH1 on 5 occassions over a 3 day period in September 1991 (folio 30 - 31: 109 - 110). He told police that read information pertaining to "patches" that is, methods of fixing routing faults.

The ramifications of the computer hacking which occurred at Northern Telecom Ltd were as follows. The company isolated its Australian subsiduary by removing its connections to Austpac* and the Internet*. Due to the extent and depth of the accessing of CORWAN by ASSANGE and the lack of information and/or records on the activities or motives of the hackers involved, Northern Telecom was forced to undertake a detailed investigation into what occurred and was forced to repair a large portion of its computer systems. This investigation was conducted to determine what had actually happened, whether the activities of these persons had had a detrimental affect on the company and finally to re-establish the integrity of its computer systems. This was done at a cost of $160,000.

(d) INCITEMENT (summary counts)

Counts 5 & 6

These counts were adjourned sine die at the Melbourne Magistrates' Court on 14.2.95. Between June 1988 - July 1991 DEDIO was involved in the writing and dissemination of information which encouraged other people to both hack and phreak.

DEDIO was the author of a 48 page manual known as the "Australian Phreakers Manual Volumes 1 - 7". DEDIO told police that he was the sole author. He said that he decided to write a magazine on how to phreak and it got so big and full of information that he was too scared to give it to anyone, and that ultimately he only gave it to 3 people, namely, ASSANGE, CARTER and s47F (folio 367 - 368). A copy of the Manual was found at Carter's premises by police. DEDIO said that some of the material was exaggerated.

The Manual's opening page is as follows:

"Introduction

This i hope will be the BE ALL and End All of Australian Phreaking Files. I started learning how to phreak about a year ago and have never looked back. I had been a fairly average hacker and I wanted to improve on it. I decided to develop my own hacking software so as to make my life easier. I wrote a Comms program which hacked out a system in 3 minutes by using default passwords, great stuff I thought. I then decided to write a Phone Sprinter to help me scan. I added a few extra function and that was the start of my phreaking career. It was during one of these scans that I came across a slight bug in the way one type of exchange talks to another but that will be explained later on. I could have missed this fault and many others if it wasn't for the way Telecom has things nice and ordered and so when they stuff up it stands out a mile. I will try to cover as much as I can on phreaking in Australia."

He later produced a second edition of the manual, which was included as part of larger computer magazine called "International Subversive". "International Subversive" was a magazine edited by ASSANGE which contained numerous articles which passed on tips on hacking. It also contained a section on pheaking which comprised the second edition of DEDIO's "Australian Phreakers Manual". The manual contained 3 chapters and was entitled "Advanced Phreakers Guide" or "How to do whatever you want on the Telephone Network". DEDIO also wrote an article for "International Subversive" entitled "Unix Shell Capture Trojan" which was an article aimed at assisting people to hack computers. Copies, of "International Subversive", or extracts thereof, were seized from the premises of ASSANGE, CARTER and DEDIO.

Dedio was also the author of a short computer file entitled "Traxbox 7" which also attempted to teach others to phreak. In this file he describes how he accidentally discovered how to phreak phonecalls. He advises his readers to try and use AXE exchanges, and nominates phone numbers to try calling and gives frequencies of the relevant tones to be played. In conclusion, after outlining various methodologies for phreaking he states:

"This method allows you to dial anywhere in the world. The number is not logged on CLI so it can't be traced and when I mean "CAN'T" I mean the following numbers couldn't pick it up.

Testing traceability
19123 CLI
55241 CLI
0173 Wake up Call
0101 [illegible]seas Call Booking

In the case of the last 2 numbers the operator wanted a number to verify as the number I was calling on wasn't on the screen. Also it will play STD pips from numbers that are STD to you. Which I found strange, it may know which exchange you are calling from as going through a Good Exchange that wasn't STD to a number I was calling still produced STD pips. This may be due to information codes sent from one Exchange to the next. I also go a Statement of Charges on my Phone and ALL the overseas calls I had made using FAO were not metered to my bill. So try your Luck!!!!"

DEDIO told police that he gave individual tuition to 5 people in how to phreak phonecalls - ASSANGE. CARTER, s47F. CONSTRUCTOR and SODABLOOM (folio 355 - 356). The intercepted telephone phonecalls of 24 October 1991 illustrates the assistance which DEDIO gave to Carter in this regard (see folios 791 - 797). Intercepted telephone phonecall of 13 October 1991 illustrates the assistance DEDIO gave ASSANGE (folio 186 - 187; 723 - 724). CARTER was never able to successfully phreak phonecalls, although ASSANGE ultimately learned to to so. DEDIO told police "Constructor went and just told everyone, after I told him not to tell anyone. So he just went and ah what's his name, s47F um, he went and just old everyone and claimed it to be his method and all that." When asked why he had disseminated the information, DEDIO told police "Ah, to show that I was capable of doing what I was doing. To sort of like big note myself basically." (folio 355 - 356)