Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:24
Received 2 June 2003

Mr J P Swindells
Assistant Commissioner
State Crime Operations Command
Queensland Police Service
GPO Box 1440
BRISBANE QLD 4001
☎07 3364 6076 07 3364 4245
E-mail:

QUEENSLAND POLICE SERVICE

STATE CRIME OPERATIONS COMMAND
7th Floor, 200 Roma Street, Brisbane, Qld 4000
Postal Address: GPO Box 1440, BRISBANE, Qld 4001

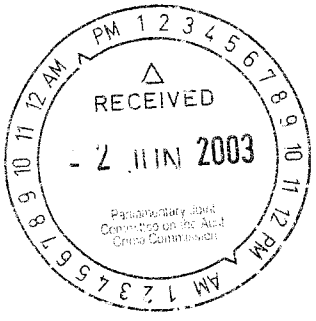
TELEPHONE (07) 3364 6076 FACSIMILE (07) 3364 4245

Our Ref: SCER 03/2220

Your Ref:

03

28 May 2003



Ms Maureen Weeks
Committee Secretary
Parliamentary Joint Committee on The Australian Crime Commission
Parliament House
CANBERRA ACT 2600

Dear Ms Maureen Weeks

I refer to correspondence inviting the Queensland Police Service to make a submission to the Parliamentary Joint Committee (PJC) on the Australian Crime Commission (ACC) Inquiry into CyberCrime.

As identified within that correspondence, a response was initially required by 9 May 2003; however, an extension was negotiated for this response to be provided by 30 May 2003.

Members of the Major Fraud Investigation Group, namely the Computer Crime Investigation Unit and the Forensic Computer Examination Unit have examined the terms of reference of the proposed inquiry on recent trends in practices and methods of cybercrime.

The Queensland Police Service has identified two distinct areas, which may be of consideration for the PJC. These areas are (i) Internet Service Providers (ISPs) and (ii) encryption and decoding.

From experiences within Queensland, particularly in relation to Internet fraud, gathering information from overseas is limited due to the necessity to serve legal documents on those Internet Service Providers away from Australia. Whilst it is recognised that the establishment of the Australian High Tech Crime Centre (AHTCC) will offer valuable assistance to these types of requests in the future, obtaining subscriber and usernames from such websites as Hotmail, Yahoo and ICQ, at the current time, is limited and not timely in nature. From experience, unless the matter is deemed urgent or some person's life is at risk, it has been found that it is not worth pursuing the involvement of the Australian Federal Police or Interpol to assist.

It is understood that an Internet Industry Association (IIA) guidelines are currently being drafted and it is reasonably expected that the establishment of these standards will also improve the reporting relationship between ISPs and law enforcement agencies. It is believed that ISPs need to verify the details of subscribers particularly the obtaining of date of birth particulars to assist in the identification process.

From a Queensland experience, persons subscribing to free mail programs/servers often use false identities to obtain a username. It has been found that some of these mail servers are overseas which thereby cause jurisdictional challenges in accessing the required information. Because these services are free, there are no checks or balances in place to ensure legitimate details are provided or more importantly, there is no requirement for these mail servers to retain information or logs.

In cases of this nature, offenders can also use proxy servers within Australia and it is almost impossible to track the identity of the sender because the ISPs have not logged the user onto their servers. Often the only way of contacting the overseas mail servers and ISPs is by e-mail and, it has been found, these persons do not respond to the inquiry. The establishment of the AHTCC may assist in this regard.

Although police may eventually identify the location where the offender has committed the offence, it is not always possible to identify the person who actually completed the computer transaction. This is a serious concern to all law enforcement agencies investigating any criminal offence involving a computer. If a Code of Practice could be implemented, this would be of benefit to this agency and other law enforcement agencies to ensure conformity in the retention of Internet Service Providers' records.

The second issue highlighted has been that of encryption and decoding. Within the child pornography area, members of the Forensic Computer Examination Unit (FCEU) have identified an increase in password protection of zip files. It is believed that as criminals become more computer literate, they are becoming more aware of available software that enables this process of concealment. The FCEU has encountered a small increase in encryption, however, it is fully believed that this issue could be an area of rapid expansion once it is more widely known that encryption is almost impossible to break.

Due to the advancement with technology, particularly the introduction of Microsoft's newest operating system, Windows 2000, it is reasonably expected that criminals will be able to easily encrypt their stored files on computers.

Australian law enforcement agencies are prepared to readily share their forensic investigative tools through the workings of the Australian High Tech Crime Managers Group (HTCMG) and the Australian Computer Crime Managers Group (ACCMG), which will now be coordinated by the establishment of the AHTCC, Australian law enforcement would benefit from a decryption capability. This capability would not only assist in the investigation of child pornography and other associated paedophile activity, but also in banking and other illegal electronic criminal investigations.

I trust this information is of assistance to you.

Yours sincerely

J P Swindells
Assistant Commissioner
STATE CRIME OPERATIONS COMMAND