Appendix 1

Examples of MPS e-Crime Cases

Example 1

Police were notified of an attack on loveandfriends.com dating site.
The hacker managed to gain control of four member profiles and deface them; he was able to do this by using an automatic dictionary attack, which guesses likely passwords of random profiles. The hacker was arrested and admitted the offences, and forensic examination of his computer revealed that he was responsible for the writing of the "MIRSA .A and MIRSA B" mass mailing worms.
These mass mailers were noted and threat assessments and alerts issued by all major anti virus companies.

He pleaded guilty to an offence under Sec 3 Computer Misuse Act 1990, and was sentenced to eight months imprisonment, suspended for two years, with a two-year supervision order.
HHJ Rivlin said it was "a very serious case, which was on the custody threshold". He also commended the investigating officers for their investigation and preparation of the case.

Example 2

A man pleaded guilty to breaking the Computer Misuse Act for sending an "email bomb" to his former employer, which caused the company's email server to collapse.

He breached section three of the Computer Misuse Act, "causing an unauthorised modification to a computer". He was sentenced at Wimbledon Youth Court to a two-month curfew and tagging order.

The man who was 16 at the time of the incident, sent about five million emails to his former employer Domestic and General Insurance, causing its email server to pack up. The messages appeared to come either from DandG staff or Bill Gates, and included a quote from horror film *The Ring*:
bUt He DoEsN't KnOw....." "He DoEsN't KnOw WhAt, SaMaRa?" "EvErYoNe WiLl SuFfEr

Initially at court the judge ruled there was no case to answer and dismissed the case on the grounds that as an email server is set up with the express purpose of receiving emails, sending it emails, albeit millions of them, could not be considered "unauthorised modification".

The Crown Prosecution Service appealed the verdict and the case was returned to Court where Lennon pleaded guilty. This created the first stated case in respect of denial of service attacks in the UK, closing a legislative gap within the current Computer Misuse Act 1990.

Example 3

The Metropolitan Police's Computer Crime Unit and Finnish law enforcement agencies arrested three men for allegedly being members of a virus-writing organised crime group.

A 63-year-old man in Ipswich, a 28-year-old man living in the Grampian region of Scotland, and a 19-year-old man in Helsinki were arrested following a global attack on computers aimed at causing infection to the machines, which would allow the team to steal personal information. Those arrested were suspected of being members of the m00p malware writing group.

Such a network could be used to spread viruses and spy ware across the Internet, without the owners of the compromised computers knowing.

Example 4

An investigation into data recovered from a computer in the United States was found to contain information from several thousand hacked personal computers in the UK. 8,500 items of personal information had been stolen by using a computer virus from UK victims.

E-mail addresses, passwords and credit card and online transaction details were part of the information recovered from the server in the United States.

Similar data relating to information stolen from 60 other countries was retrieved. Prevention measures taken by police working in partnership with law enforcement and industry were instigated to prevent any of the compromised data being used.

Example 5

This case concerns a Botnet investigation jointly conducted by the Metropolitan Police, Federal Bureau of Investigation (FBI) Seattle Field Division and Headquarters Division Royal Canadian Mounted Police (RCMP). The Computer Crime Unit were contacted by a major UK Internet Service Provider (ISP) regarding a Botnet consisting of approximately 19,000 infected host computers. A compromised server located in Acton was controlling the infected computers. This computer was taken off line and the suspects switched the BotNet to a compromised server in Germany. Over the next 72 hours the suspects moved the Botnet to the United States, Korea and finally back to the US where it was dismantled. UK enquiries revealed that there was a Canadian suspect involved located in the Toronto area. Analysis of the computer virus demonstrated that the Botnet was intended to generate spam mail. Canadian authorities were notified and a joint operation initiated.

At the same time it became apparent that the FBI were investigating a similar Botnet case involving the same suspects. In this instance the Botnet was designed to steal passwords from infected computers. Turner and his cousin were arrested following a surveillance operation. Following further investigation

the second suspect was eliminated from the enquiry. Turner, a computer science student admitted modifying pre-existing computer viruses and using them in the Botnets, he also admitted causing unauthorised access to the compromised servers in order to control the Botnets.

The damage in computer downtime was put at approximately £58,000. During this investigation the Metropolitan Police computer crime unit initiated informal police to police enquiries with German, Norwegian, Australian, Korean, US, Brazilian and Canadian Police agencies.

Child Abuse Investigation Command

Example 6
Allegation of rape by 14-year-old stepdaughter. Five computers, two cameras and numerous disks submitted for examination. Examination identified indecent images of victim including deleted images. Emails between the two parties also recovered. Suspect recently pleaded guilty to 11 counts rape, four counts sexual activity with a child, one count of indecent assault and possession of indecent images up to level four.

The viewing of video-cassettes continues to reveal offences of possession of indecent images and 'Hands On' child sexual abuse. One homemade videocassette was identified whereby a 17-year-old female was being raped. Through this evidence the CAIT officers were able to identify the girl who had been raped 16 years ago. Awaits trial having pleaded guilty to possession of indecent images.

Example 7
Detained at Heathrow following seizure of imported CD ROMs. Computer equipment and other media examined. Evidence found of suspect sexually abusing young boys in Africa and England. Victims identified in both Africa and England. Suspect charged with three counts of rape, three counts of attempted rape, one count of administering a substance with intent and taking and possession indecent images of children. Pleaded guilty and sentenced to a minimum of 6 years imprisonment.

Covert Internet Investigations (CII)

Through the use of an authorised Covert Internet Investigator over a 9-month period 475 people communicated with the CII through social networking groups, knowing that the profile was that of a young girl. These suspects were keen to speak with, travel and have sex with the young girl. The CII progressed the investigation and engaged 175 suspects in Yahoo or MSN. To date 16 have been arrested with a further nine to be arrested in the very near future and intelligence to be disseminated to other forces. An early example and success was in April 2006. A male travelled from Uxbridge to Upminster in the belief that

he would meet a 12 year old girl. He had a number of DVDs and a player for the girl to watch. She would then have to copy the same sexual acts. He also travelled with towels, flannel, and baby lotion and hotel key card. The DVDs contained indecent images level one - five. Charged with attempting to meet a girl under 16 following sexual grooming, Attempting/incite girl under 13 to engage in sexual activity, Distribution/Making and Possession of indecent images. At Middlesex Guildhall given indeterminate sentence with a minimum of 30 months concurrent and disqualified with working with children. The computer forensics in this case started on the day to allow for the suspect to be charged the following day.

Assistance to Cambridgeshire

On two separate occasions the Pro-active unit has given CII assistance to Cambridgeshire Constabulary. First case brother of a 12-year-old girl noted that she had been communicating with a 17-year-old boy. Mother informed and local police called. CII was able to take over the role/profile of the girl and continue communicating with suspect. The suspect was identified as being in Cambridgeshire. Arrested charged with grooming offences, pleaded guilty and sentenced to four years imprisonment. Suspect was actually 63 years old. Second case mother walked into girl's bedroom and saw a 30-year-old male on her web cam. Police called and CII deployed. CII assumed girl's identity and suspect arrested in seven days for grooming offences. Suspect lived only 250 yards from the victims address. When taking over a profile the CII has to understand how the language previously used and what the victim has previously disclosed to the suspect.