

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 177

Senator Ludwig asked the following question at the hearing on 24 May 2005:

- a) To what extent does the AFP work with Australian IT industry stakeholders in determining policy on cybercrime?
 - (i) If so, which ones?
- b) Has the AFP conducted any investigations into internet 'phishing' in Australia?
 - (i) If so, have any charges been laid, and have any convictions been recorded?
- c) Have any phishing websites been found to have been operating from inside Australia?
- d) Have the AFP conducted any investigations into denial-of-service extortion or attacks in Australia?
 - (i) If so, have any charges been laid, and have any convictions been recorded?
- e) Have any Denial of Service groups been found to have been operating from inside Australia?
- f) Has the AFP conducted any investigations into extortion crimes that are conducted over the internet?
 - (i) If so, have any charges been laid, and have any convictions been recorded?
- g) Is the AFP involved in any international investigations or task forces in relation to either of the above two offences?
 - (i) If so, please provide details.
- h) Has the AFP conducted any investigations into computer virus production in Australia?
 - (i) If so, have any charges been laid, and have any convictions been recorded?

The answer to the honourable senator's question is as follows:

- a) Responsibility for cybercrime policy rests with the Attorney-General's Department. The Department consults the AFP and the AHTCC on any policy changes that are relevant to law enforcement. The AHTCC is actively involved in a number of inter-governmental groups and industry fora where cybercrime policy is discussed.
- b) Yes.
 - (i). 3 people have been charged, one of these people have had a conviction recorded and was ordered to be of good behaviour for 18 months; another was ordered to be of good behaviour for 12 months without a conviction recorded. The third person is currently before the Courts.
- c) Yes. The AHTCC has discovered one phishing site which was hosted on a compromised computer in Australia. The owner of this computer was unaware that this illegal activity was taking place.

d) Yes.

(i) No.

e) Yes, the AHTCC is currently investigating an offence of this nature.

f) No.

g) Yes.

(i) The AHTCC works closely with international law enforcement agencies to investigate instances of cybercrime which impact on Australia, but are perpetrated offshore. For example, the AHTCC has strong bi-lateral links with the United Kingdom's National Hi-Tech Crime Unit and similar international law enforcement agencies.

h) Yes. The AFP, through the AHTCC, is currently investigating an offence of this nature.

(i) No charges have yet been laid, however the investigation is ongoing.