Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:8
Received 9 May 2003

Dr Patrick J Forde
Curtin Business School
Curtin University of Technology
GPO Box U1987
PERTH WA 6845
☎08 9266 7797 08 9266 2378
E-mail: fordep@cbs.curtin.edu.au

Dr Patrick J Forde
Curtin Business School
Curtin University of Technology
GPO Box U1987
Perth
Western Australia 6845

8th May 2003

The Secretary
Parliamentary Joint Committee on the Australian Crime Commission
Suite S1 107
Parliament House
Canberra ACT 2600

Paedophile Utilisation of Anonymous Cyber Practice

Dear Sir/Madam

This submission to the Parliamentary Joint Committee on the Australian Crime Commission under paragraph 55(1)(d) of the *Australian Crime Commission Act 2002* addresses the issue of paedophile utilisation of anonymous cyber practices.

Illegal and objectionable Internet activities can be rendered effectively anonymous using established techniques (e.g., email remailers) or evolving techniques (e.g., hidden peer-to-peer networks). Research into paedophile Internet practice has shown that perpetrators will take advantage of these methods in order to facilitate their activities (see the Australian Institute of Criminology: http://www.aic.gov.au/publications/tandi/tandi97.html). These practices require an advanced level of applied Internet knowledge and an ability to be up-to-date with the latest developments. Paedophiles use the Internet to create worldwide communities that disseminate knowledge about anonymity and other security matters. Government agencies need to be informed about current paedophile Internet practice in order that computer forensic evidence can be fully utilised during prosecution. Covert or real-time operations would also benefit from an awareness of paedophile Internet practice. In addition, this knowledge would be useful in areas other than the pursuit of paedophiles (i.e., when terrorists, money launderers and other criminals seek to mask their Internet activities).

FreeNet is an example of a recently activated anonymous network that was constructed to protect the identity of all network interactions. Users, 'www type' page sites and data files were designed so that the initiator of these transactions would be kept anonymous. Indeed, this network was constructed to exist underneath the normal structure of the Internet and is therefore invisible to most Internet users. While it must be stated that FreeNet is an experimental environment that was developed to facilitate free speech and that it has recently experienced a number of difficulties, its design is openly

available to communities interested in anonymity. In fact, paedophiles have already invaded the experimental environment despite the attempts of the originators to self regulate this network.

Knowledge about anonymous Internet practices contemporaneously applied within communities conducting illegal or objectionable activities should be routinely collected. Furthermore, this understanding should be accessible to government agencies.

Consequently, Parliamentary support and encouragement is requested to consider the assembly of a pragmatic environment (based on the participation of government officers and academics) whereby knowledge about anonymous Internet practices can be accumulated and distributed. Such an environment could also provide training experiences for authorised officers.

A more detailed explanation of this 'pragmatic environment' can be presented upon request.

Yours faithfully

Paddy

Patrick J Forde