Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:22
Received 2 June 2003

Mr Brendan Scott
141 Station Street
NEWTOWN NSW 2042
☎
E-mail:
brendanscott@optusnet.com.au

From: Brendan Scott [brendanscott@optusnet.com.au]
Sent: Sunday, 1 June 2003 4:04 AM
To: ACC, Committee (SEN)
Subject: Submission to Cybercrime legislation

Brendan Scott
141 Station Street
Newtown 2042

To: The Secretary
Parliamentary Joint Committee
Inquiry into Cybercrime

Dear Secretary

Submission to PJC Inquiry into Cybercrime Legislation.

I do not have specific expertise in relation to the three headings listed in the terms of reference for the current
Cybercrime Inquiry. As such, I would like to make some short comments at a general level of the concerns that I have
with the Cybercrime Act, and its related State legislation.

My main concerns with the legislation are:

(1) the concept of authorisation in relation to data. This of itself presupposes a concept of property in data (in order to identify the person qualified to give an authorisation). While there are many lobbyists who argue that there ought to be property in data, such a concept does not exist in Australian law. The Cybercrime legislation effectively makes a great deal of assumptions about policy issues relating to the control, distribution and dissemination of data.
It in effect creates many of the characteristics of a property right without adequate policy discussion. In my view the
assumptions the legislation makes are inimical to my understanding not only of civil liberty, but also of the minimum
level of access to information which is necessary for a functional civil society and the optimal operation of Australia
in an information economy. Indeed, there is mounting evidence to suggest that the information economy is a form of "reverse commons" in which access and distribution should not be unduly restricted if optimal economic potential is to
be reached; and

(2) breadth. My view of the Cybercrime legislation is that it is overbroad in its reach. I drafted a submission for the
NSW Society for Computers and the Law when the legislation was being considered in parliament. In that submission I
outlined a number of areas where the reach of the legislation was too great. When I raise this criticism with
participants in the criminal justice system they explain that there are checks and balances, and part of those checks

and balances are the discretion of the courts and of the relevant director of prosecutions. It is disconcerting that
legislation creating overbroad criminality is justified effectively on the basis that it won't be enforced or won't be
fully enforced or that it would be too difficult to draft properly targeted crimes. In my view, the cybercrime
legislation makes illegal a broad range of activities which persons would not ordinarily consider criminal, with
technically the only thing lying between reasonable acts and criminality being an executive or judicial discretion.

(3) inappropriate drivers. My experience in watching the computer security industry and advising my clients in relation
to it is that much policy making in this area is driven by vendors with a solution attempting to generate a problem (PKI
at its worst is an example, although digital signature scare tactics have subsided in recent years). I am concerned
that crimes are being created without due consideration of the adequacy either of existing provisions or of clarifying
the application of those existing provisions.

I am willing to provide more details on any of these points on request.

Yours faithfully

Brendan Scott

Brendan Scott is a lawyer practising in IT and telecommunications law in Sydney. Brendan is the immediate past
president of the NSW Society for Computers and the Law.