Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:22A
Received 7 September 2003

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

Parliamentary Joint Committee

on the Australian Crime Commission

Cybercrime Inquiry

Supplementary Submission

Brendan Scott

6 September 2003

Purpose

1. The purpose of this supplementary submission is:

   (a) to identify a circumstance in which the *Cybercrime Act* has a direct and real impact on the conduct of my business;

   (b) to suggest changes to the legislation to address in the short term some of the issues I have raised.

Statement of Principle

2. During my giving of evidence on 18 July the Joint Committee asked for what could be done to remedy the problems I see to exist with the Act. In my view the Act as a whole needs to be rethought. As I stated, I believe it is not appropriate to criminalise access to data merely on the basis there is some form of access restriction in respect of that data. I understand a rethinking of the Act is probably impractical given the current circumstances. It may be more pragmatic for a more thorough review of the operation of the Act be carried out in a number of years where more evidence of other aspects of its application are available.

Proposed Changes to the Act

3. I have given further thought to how some of the problems I have raised might be addressed. In particular:

   (a) any access to restricted data should not be criminal unless the relevant access control system is subverted in the course of that access;

   (b) (related to (a)) circumstances which relate to "access" to restricted data should only be crimes where the access which occurs is the type of access actually restricted by the access control system. For example, if the access control system restricts only viewing the data it should not be a crime to copy the data (and vice versa).

   (c) the definition of "restricted data" should be limited to data "access to which can only be achieved through complying with an access control system associated with a function of the computer".

   (d) Section 476.2, should be clarified to state that a person who lawfully possesses a computer or data storage device on which data is held, is entitled to cause any access to, modification of or impairment of that data. Similarly for the impairment of communications to and from equipment that is lawfully possessed. I ought to be able to wipe my own mastercard for example (even though the bank may assert ownership over the card itself).

4. It could be argued that item 3(d) may allow a person to "slip through the net" of the Act by copying data to their own computer and then accessing it. However, the transfer of the information to their computer in the first place will likely be a crime; and where the data is

resident on a person's computer there are no consequences for any other person arising as an immediate result of their access to or modification of that data (although subsequent crimes may be committed as a consequence of that access if, for example, they then copy that modified data elsewhere). In my view this additional clarity will provide a real benefit without any practical detriment.

Real World Worked Example

(To understand this example you will need to work from a soft copy of this document and Microsoft Word. This example also assumes that one of the constitutional qualifiers on each of the offences is met (eg a Commonwealth computer is involved)).

5. During the course of my evidence the Joint Parliamentary Committee indicated that on one view the arguments I raised in my submission and in my evidence were of a theoretical nature. I wanted to provide a "real world" example where the legislation would inappropriately criminalise an ordinary action in an everyday office environment.

6. This submission has been created in Word for Windows, a part of the Office XP package and sent to the Joint Parliamentary Committee in a Word ".doc" format. One of the functions of Word is the ability to "protect" a document. Protection has been applied to this document with a password (you may notice a number of the icons in Word's toolbar are greyed out). While a document is protected, the data in that document can be viewed. However, the data in the document cannot be moved or copied (at least from within Word). In this submission data cannot be moved or copied (for example, try to select and copy this paragraph).

7. The data in this submission is therefore data "to which access [which includes copying or moving of data s. 476.1] is restricted by an access control system associated with a function of the computer" – it is "restricted data" within the meaning of s 478.2.

8. Documents are sent with this protection from time to time in the course of legal practice. The apparent purpose of protecting documents in this manner is to gain an inappropriate negotiation advantage by making it difficult for the other side to respond to the wording in an agreement. Rather than marking the document up they need to respond in a cumbersome "add the following words to clause x after the occurrence of y" format, equally they are unable to use electronic facilities to search through the document. This allows one side to "retain control" of the document. Having to comply with this form of protection increases time (eg manual searching for references and indirect modifications) and therefore cost with no social benefit.

9. This "protection" can be removed even where the password for the document is not known through the use of the Word program by the following steps:

   (a) open the "save as" dialog (File menu-> Save As)

   (b) in the "save as type" dropdown box, select "Rich Text Format (*.rtf)"

   (c) click "Save"

   (d) close all open documents.

   (e) open the file as saved (*.rtf)

   (f) Now choose Tools -> Unprotect Document.

10. I authorise the Parliamentary Joint Committee on the Australian Crime Commission, each of its members and its secretariat to make any access to or modification of any copy of this submission held by or on behalf of the Parliamentary Joint Committee on the Australian Crime Commission and its secretariat.

11. Please verify the removal of protection by carrying out the steps set out in paragraph 9 then selecting and copying a paragraph from this submission into another document.

12. I am concerned that the application of this procedure, without the appropriate authorisation (as I mentioned in my evidence, it is not clear who has the power to grant such an authorisation), will be a breach of section 478.2 of the *Criminal Code*. I would typically encounter a number of documents with this kind of protection each year.

13. This example illustrates some of the problems with the definitions of "access" and "restricted data".

14. In my view it would be inappropriate if the application of this procedure constituted a criminal offence regardless of whether the person who created or disseminated the document had authorised such an application.

Brendan Scott

141 Station Street

Newtown 2042