Graeme McGowan
Covert Investigations Policy Team
Home Office
5th Floor, Peel Building
2 Marsham Street
London SW1P 4DF

28th July, 2006

Dear Graeme McGowan

Re: Public Consultation – The Investigation of Protected Electronic Information

It seems fairly obvious that if someone has taken the trouble to protect or encrypt material it is very likely they have done so precisely in order to keep the material secret. That is the whole point of protection and encryption after all. However, where such a person is suspected of, and is being investigated in relation to, the possession of indecent images of children, or other crimes against children, we think it is imperative that the contents of any encrypted material found in the person's possession can be viewed by the investigating officers, and as soon as possible. Were it to be otherwise, not only might important information relating to the matter being investigated remain unavailable to the police, but details of other crimes might well remain concealed, as might the identity of as yet unknown victims and abusers.

At the moment, under s. 53, RIPA, 2000, the potential penalty for refusing to decrypt material is a maximum prison sentence of two years. Thus the problem is obvious. If the person suspected of possessing indecent images believes that disclosing what is in the encrypted files could render them liable to a harsher penalty of some kind, then logically they will opt for the lighter sentence and they will therefore ensure that potentially much worse crimes remain undiscovered and not investigated. Inter alia, this could put more children at risk of abuse in the future.

The consultation document provides several examples of cases where law enforcement were unable to see computer files because they had been encrypted and no key was available to decrypt them. The circumstances suggest that the contents of the encrypted files were very likely to contain materials or information relating to child sex abuse or child sex abuse images.

85 HIGHBURY PARK • LONDON • N5 1UD
TEL 020 7704 7159 • FAX: 07092 191249
EMAIL JOHN.NCH@BTOPENWORLD.COM

Typically in many child sex offence cases or in cases relating to the possession of indecent images of children, the sentencing options available to the courts greatly exceed the two year maximum currently available, under s. 53, RIPA, 2000. In that light, to answer question 19 (v) of the consultation document, we think two years is very likely to be an insufficient maximum deterrent and it ought to be increased.

Paragraph 19 (vi) then asks what we think the new maximum sentence should be.

The circumstances outlined in paragraph 17 of the consultation document provide four different scenarios: one where there is direct evidence of what is contained in the encrypted files e.g. from a witness. Scenarios are also given where there is indirect evidence of what the encrypted file or files might contain:

(1) the person in possession has previous convictions for child pornography offences
(2) there are indecent images of children on the same computer or on the same disk as the encrypted data
(3) there are indecent images of children in a different computer or on a different disk seized at the same time

If the person can produce evidence to show that the encrypted files do not contain illegal materials, or if the court is satisfied that the person genuinely cannot decrypt the file, for example because they have lost or never had the key, the question ceases to have any relevance. The matter will not be pursued. But otherwise, bearing in mind that it will always be open to the person found in possession of the encrypted file to decrypt them and show what they actually contain, we can see no reason why, in the circumstances outlined in paragraph 17 of the consultation document, the courts should not have available to them all of the sentencing powers they would have had if the material was what the prosecution established it was very likely to be. This means that, potentially, the courts would be able to give up to 10 years imprisonment.

We would now like to raise a related point, which is not directly addressed in the consultation document.

The logic of the new powers proposed to deal with encrypted material is that society cannot allow people to deploy technical solutions to put themselves beyond the possibility of being held to account in the courts for their actions.

But here is another, very similar scenario. Go into any newsagent's shop on any day of the week and look at the "free" CDs attached to the covers of most of the computer magazines on display. The chances are that one or more of them will feature giveaway versions of fully-working software with names like "Evidence Eliminator" or something similar.

The purpose of these programmes is not disguised in any way. Quite simply they do multiple wipes of all or part of a computer hard drive. This "eliminates" any "evidence" of anything and everything that has been performed on that computer that the owner does not want anyone else to see. If the computer has been used in the commission of a crime, for practical purposes it makes it impossible for law enforcement to recover anything of value that could be produced in a court. There has

been at least one case in the UK where no serious charges could be brought against the defendant precisely because he had routinely deployed such a product, yet through effective intelligence gathering the police knew exactly what he had been doing.

There are, of course, entirely legitimate reasons why people might need, occasionally, to do a thorough wipe of a hard drive, with a programme such as “Evidence Eliminator”. For example, if one intended to donate, say, an older computer to a relative or friend or to charity, one would want to ensue that, whether by accident or design, no one could recover any personal or confidential information that might previously have been kept on it.

But one has to wonder why someone would want to use a programme like "Evidence Eliminator" every day. We think it is irresponsible of the computer magazines, essentially, to promote and advertise software of this kind in the way that they do: it's a bit like placing an advertisement to say something like" If you want to break the law and get away with it, we've got just the thing for you!" Perhaps the seasoned criminal will already have programmes of this kind or know where to get them, but why put them on the shelves of W H Smith and thereby, perhaps, draw them to the attention of fledgling or opportunist criminals?

Might there be a case, therefore, for saying, as with the proposals on encryption, that where it can be shown that a person suspected of possessing indecent images has used a programme like "Evidence Eliminator" to wipe everything from their hard drive, yet the police are in possession of information which shows, to the satisfaction of a judge, what he had been doing with his computer prior to that, the normal rules of evidence can be relaxed in some way?

An alternative approach might be to make it a crime, at least for persons with relevant prior convictions, to possess or use such programmes and merely finding them with a programme of that nature on their computer or in their possession would be enough to constitute an offence.

Yours sincerely,

Executive Secretary