Submissions on the Report of the Inter-departmental Working Group on Computer Related Crime by the Criminal Law & Procedure Committee of The Law Society

The Society's Criminal Law & Procedure Committee has preliminarily reviewed the various recommendations made by the Inter-departmental Working Group in its Report on Computer Related Crime. While the Committee welcomes most of the recommendations put forward in the Report, it has the following concerns:

1. ***Jurisdiction***

The Working Party has made various recommendations regarding the jurisdictional issue. One recommendation is to expand the Hong Kong jurisdictional net regarding the offence of "*obtaining access to a computer with intent to commit an offence*" so that Hong Kong courts would have jurisdiction if the computer to which access is obtained for committing the offence is in Hong Kong. This would appear to catch the distributor of a virus that is causing damage in Hong Kong.

In order to ensure that this proposal will have the desired effect, **the Committee recommends that that it should be made clear that access to a computer includes access to files stored on the machine. The Committee further believes that there should be appropriate extradition provisions at the international level to strengthen the Working Party's various proposals.**

2. ***Encryption***

The Working Party has recommended that appropriate legislation be introduced to enable law enforcement agencies to be provided with decryption tools and decrypted text when necessary and justified.

In deciding whether such investigatory powers should be given to the law enforcement agencies and the scope and manner of exercising such power, the Committee has the following concerns:

(a) implications of the proposed legislation on the development of e-commerce;
(b) potential infringements of privacy;
(c) implications for the disclosure of encrypted information, which may include legally privileged information;
(d) the right of individuals against self-incrimination,
(e) the need for disclosure of keys when access to plain text would be sufficient; and
(f) the need for the empowered agencies to be fully accountable to democratic institutions and subject to public scrutiny.

It should be noted also that cryptography is usually used to thwart criminals rather than to help them and care should be exercised before breaking security.

The Committee recommends that the following safeguards be embodied in the proposed legislation regarding access to encryption keys:

(a) there should be disclosure only where obtaining the key is really necessary;

(b) disclosure should be "*proportionate*" to what might be achieved;

(c) there should be provisions for the protection of the relationship between solicitors and clients;

(d) there should be provision for the destruction of the encrypted information once it is obtained; and

(e) there should be a right to sue law enforcement agencies if any material is leaked as a result of the negligence of the law enforcement agencies

The Committee observes that the Working Party's proposals for access to encryption keys may be outdated. The proposals are confined to encryption but other encoding techniques are already available such as biometrics, where identification is based on the biological and behavioural characteristics of individuals or quantum cryptography, which no longer relies on keys. With this technique messages are sent using photons of different polarities. Attempts to observe signals irrevocably alter the polarity of many photons and destroy the message before it can even be read. **The Committee recommends that the proposal should be updated to embrace other encoding techniques.**

There is a further concern with the way the law enforcement agencies are presently seizing computers for evidence and investigation purpose. It is observed that under the current practice, enforcement agencies would seize the entire set of computer hardware that causes tremendous and unnecessary inconvenience sometimes resulting in the collapse of businesses. **The Committee recommends that sufficient safeguards be introduced to the current system, in particular, requiring a warrant to specify the ambit of what is to be seized from a particular hard disk of a computer.**

3. ***Penalties for Offenders***

The Working Party has recommended increases in the penalties for several computer-related offences without giving any information on the different age groups of offenders involved. To consider whether such increases are appropriate, **the Committee would urge the Administration to provide statistical information setting out the age groups of the offenders committing these computer-related offences.**

The Criminal Law & Procedure Committee
The Law Society of Hong Kong
9 February 2001