person who took part in the raid earlier this year on the Golden Arcade (the centre of illegal software distribution in Hong Kong). The raid has resulted in charges being laid against approximately 20 people. A visit to the arcade, however, revealed that business is still booming. Probably 100 shops were offering manuals and discs for sale with no pretence that they were anything other han pirate. There must be money in piracy; one of my fellow delegates purchased a large amount of pirate software to take back to the US to show his clients. A chance meeting on the street an hour later with the couple who were serving in the shop resulted in an invitation to dinner at their very nice new apartment. Our hosts wore what must be one of the few genuine Rolex watches in Hong Kong.

It is certain that Asia is becoming ever more aware of the problems associated with intellectual property protection of computer products. The needs as well as the practical difficulties of enforcement and the economic consequences of doing so are all being thoroughly examined.
Jim FitzSimmons

VICTORIA HACKS BACK

CRIMES (COMPUTERS) ACT 1987

The Victorian Parliament passed a Bill on 24 May 1988 amending the Crimes and Summary Offences Acts to make certain further provisions for offences relating to the manipulation of computers and other machines and the falsification of documents. This Act is yet to be proclaimed but is expected to be in force by the end of the year.

INTRODUCTION

The main purposes of the Crimes (Computers) Act ("the Act") are to:

1. ensure that major fraud offences apply to conduct involving not only dishonest manipulation of the traditional written documents but also of articles and documents produced by or stored in computers or other machines;

2. create new offences covering the falsification of computer related articles such as computer stored records, disks, tapes and automatic teller machine cards (ATM cards) and of other instruments not in "written form";

3. create a new offence relating the innocent but unauthorised entry into computers i.e. "hacking";

FRAUD AND BLACKMAIL USING COMPUTERS

The Victorian Government has taken into account the extensive reports prepared on the subject of computer related crime by the Tasmanian Law Reform Commission, the standing Committee of Attorneys General, the Queensland Government's proposed Green Paper, the Scottish Law Commission's paper and the OECD's report outlining the consideration given to these issues in the 12 other Western European countries. The striking feature emerging from these analyses was that the overwhelming majority of activities commonly thought of as computer related crimes were adequately dealt with by existing criminal offences carrying substantial penalties. Traditional offences such as theft, criminal damage, obtaining by deception and false accounting, some of which have been known to the law for centuries, were thought to be readily applicable to offences involving even the most modern technology.

The Victorian Government saw the main difficulty with the present criminal law in relation to computer fraud as being the many narrow legal rulings of the meaning of "deception". The existing major fraud offences in the Crimes Act such as dishonestly obtaining property or a financial advantage by deception require proof of "deception" as an element of the offence. There exists some doubt as to whether this term in its ordinary meaning was wide enough to cover behaviour involving deception directed initially not at another person but at a computer or other "machine". It was noted that some prosecutions in England have failed for this reason.

Indeed there are where

machines such as ATMs, slot machines and turnstiles perform functions previously carried out by people such as bank tellers, shop assistants or gate keepers. It was thought to be anomalous if a dishonest transaction perpetrated directly against another person amounted to an offence but a similar transaction involving the manipulation or misuse of a computer or machine did not.

The Act therefore makes it clear that fraud offences will apply whether the dishonest transaction has as its immediate object a computer, a machine or a person.

As well, definitions contained in the Act draw on the very wide definition contained in Section 38 of the Interpretation of Legislation Act 1984 which extends the notion of a "document" to embrace a wide range of articles including any device in which data is embodied so as to be capable of being reproduced therefrom and anything on which is marked any words or figures capable of carrying a definite meaning.

HACKING

Initially the Bill did not address the subject of computer hacking where there was no element of dishonesty in obtaining property or financial advantage or in falsifying or damaging data. Hackers who did gain unauthorised access to a computer system with a view to altering or deleting data could have been prosecuted for the falsification of documents or for criminal damage. The hacker who intended to dishonestly obtain the free use of a computer system for which payment was normally required would be guilty of the offence of obtaining financial advantage by deception. These offences involve criminal intent and harmful consequences and it was thought by the Victorian Government that a specific offence for "innocent" hacking should not be created which would attract criminal penalties. The Government considered that unauthorised use or access in relation only to certain types of information should be the subject of criminal penalties but wished to delay consideration of this aspect further. However, as a result of pressure from the Victorian Opposition, in its final form the Act amends the Summary Offences Act by inserting a section "Computer Trespass" which deals with this. Section 9A states that a person "must not gain access to or enter a computer system or part of a computer system without lawful authority to do so". The penalty for this includes 6 months imprisonment.

EXTRATERRITORIALITY

Finally, the Act seeks to address what is becoming a common problem in situations where there is cross–border computer communications. The Act purports to allow proceedings to be commenced in Victoria where there is a "real and substantial" link between on the one part the act or thing done either outside or partly outside Victoria and on the other the State of Victoria. "Real and substantial" is further defined to include situations where a significant part of the conduct or the doing of the act or thing occurred in Victoria or where the act or thing done was outside Victoria but with the intention that substantial harmful effects should arise in Victoria. It is stated that this section would address the anomaly where you had all of the preparatory steps towards the commission of an offence occurring in the State, the offender not leaving the State, the harmful effects of the offence occurring within the State and the proceeds of the offence returning to the State yet because the final element of the offence did not occur in that State then that offence could not be dealt with in that State.

SUMMARY

In summary then the Act reinforces those criminal offences already existing which deal with certain computer related crimes especially where there is damage caused or property or financial gain fraudulently or dishonestly obtained. The Act does this by extending the concept of "deception" to include fraud and blackmail or the causing of prejudice to another person where such conduct is initially directed at or involves the use of computers, machines or computer generated or stored articles. The Act also creates an offence for "innocent hacking" with a penalty including six months imprisonment. Finally, the Act attempts to counter the jurisdictional difficulties presently experienced where cross boundary communication systems are used in computer related crimes. It does this by allowing prosecutions to be brought in Victoria where there is a "real and substantial" link between the offence and the State.