

Computer Crime: New Queensland Offences Relating to Computers

by John Miller

In April 1990 the Criminal Code Review Committee was established and charged with the task of comprehensively reviewing the Queensland Criminal Code. Within the purview of the Committee constituted by Mr Rob O'Regan QC, Mr James Herlihy and Mr Michael Quinn was the deficiency in the current Criminal Code in relation to computer crime. In its final report forwarded to the Attorney General in June, 1992 the Committee recommended that the following section, derived from section 440A Criminal Code (WA), be incorporated into the Criminal Code:

s228 Unlawful operation of a computer system.

- (1.) In this section -
- (a) 'system' means a computer, computer system, computer network or a part thereof;
- (b) a system is a restricted-access system if:-
- (i) the use of a mechanical device or a particular code, or set of codes, of electronic impulses is necessary in order to obtain access to information stored in the system or operate the system in some other way; and
- (ii) the person who is entitled to control the use of the system has withheld access to the mechanical device or knowledge of

the code, or set of codes, or the means of producing it, to a particular authorised person or class of authorised persons.

- (2.) A person who without proper authorisation -
- (a) gains access to information stored in a restricted-access system; or
- (b) operates a restricted-access system in some other way, is guilty of a crime and is liable to imprisonment for one year.
- (3.) If an offence against Subsection (2) is committed in circumstances where the offender has an intent to defraud any person or an intent to cause criminal damage, the offender is liable to imprisonment for three years.

The Committee was of the opinion that the present law was deficient in three particular respects namely:

1. the 'theft' of information stored on computer;
2. damaged caused to a computer that does not involve physical damage (for example erasure); and
3. unauthorised access to a computer system. (Final report of the Criminal Code Review Committee to the Attorney-General, June 1992.)

The proposed section specifically targets unlawful access to computers, making it a specific offence for the first time in Queensland. The Committee was of the view that the solution to the problem in respect of theft of confidential information

stored on computer lay in proscribing "unauthorised access" to the computer system because there were conflicting decisions as to whether confidential information was 'property' and therefore capable of being stolen. The Review Committee also recommended introducing an aggravated form of the offence, subsection (3), to recognise the increased seriousness of unauthorised access gained with intent to defraud or to cause criminal damage.

By providing that the offence is committed upon unauthorised access being gained to a computer system the scope of the offence is extremely wide.

Unauthorised Access

A breach of 'in-house' regulations may not be sufficient to sustain a charge under this provision. In *Lynn v Barylak*, (Victorian County Court, 7 February 1991), Australia's first computer virus prosecution the issue was whether the accused had gained 'unauthorised access to a computer system'. The accused was a student at the Swinburne Institute of Technology in Melbourne. The substance of the charge was that he had been involved in spreading a virus through the use of an unauthorised diskette. A new procedure was introduced by the Institute to ensure that only clean diskettes were used to boot the machines on the network. In order to use boot diskettes, students were required to collect the diskettes from senior students to return them once their session was complete. The accused was observed using a non-standard diskette which was later seized from

his house and he was subsequently charged. It was argued that the defendant did not lack "lawful authority" to access the system because as an enrolled student he had access to the Institute's computers and there had been a flouting of procedural requirements by many students who used their own diskettes for reasons of convenience. The prosecution argued that if the accused had been attempting to spread a virus then his authority to use the system did not extend to access for that type of activity. The prosecution conceded that a breach of 'in-house' rules in itself did not deprive a person of lawful authority to access the computer. Ultimately the prosecution failed to prove that the accused had acted with the intent of introducing the virus and accordingly the charge was dismissed.

Piracy

It is doubtful whether the proposed section would cover an act of piracy, that is, the unauthorised copying of a computer software program as that act is not gaining access to a "restricted-access system" within the

meaning of that term. It is doubtful whether the offence of stealing would cover this as what is being taken is the intellectual property which the Review Committee themselves have conceded is outside the traditional definition of 'property' and therefore not capable of being stolen. The owners of software programs would of course have civil remedies against pirates, however, the section is deficient in that piracy is not made a criminal offence and is disappointing for software owners as the potential to save on the cost and time involved in bringing a civil action is lost.

Criminal Damage

The proposed section would undoubtedly cover the situation of criminal damage where for instance an accused had deleted and added files, put on messages, made sets of his own users and operated them for his own purpose, and changed the passwords of authorised users even though the computer disks affected were despite the accused's action still capable of performing the functions they were designed to perform. This

was because the accused it was held had altered the particles on the computer disks in such a way as to cause the impairment of the value or usefulness of the disk to the owner. *R v Whiteley* (1991) 93Cr.App.R.25.

Further, it has been held that a defendant who deliberately erased a computer program from the plastic circuit card of a computerised saw so as to render the saw inoperable had caused 'damage' as what had been done by the defendant's action had made it necessary for time, labour and money to be expended in order to replace the relevant programs on the printed circuit cards. *Cox v Riley* (1986) 83Cr.App.R.54.

Conclusion

The proposed section is a timely amendment to the Criminal Code which was drafted before the advent of the motor vehicle let alone the computer. The law must keep pace with the increasingly sophisticated criminal in a technological society. The legislating of this new section is undoubtedly a step towards this. ❧

John Miller is a solicitor with Bilshenan & Luton, Brisbane.

Press Release

FaxLaw - Legal Information Tailored to Your Needs

FaxLaw, a new service recently launched by Butterworths (legal tax and commercial publishers), is an example of the way in which computer technology can be used to bring flexibility to a publication. Each subscriber is able to act as their own publisher, by tailoring the information to suit their individual needs.

FaxLaw encompasses summaries of all superior court decisions as well as new statutes, regulations and leg-

islation for both the state and federal governments.

Subscribers select up to six topics on which they wish to receive current information on a weekly basis. Butterworths' unique computer system then creates a customised issue for each subscriber by selecting the appropriate topics from its extensive database, and this is automatically faxed to the subscriber.

'This service is the most sophisticated legal publication available in

Australia today', says Alistair McLean, Product Manager for Electronic Publishing at Butterworths. 'Only FaxLaw offers subscribers the opportunity to select the subjects they are interested in, and combines this flexibility with the speed and accuracy of electronic publishing.'

'The next step is to eliminate paper completely, and FaxLaw will soon be available for computer networks. Information will be sent directly from the Butterworths' database to