The First Computer Virus Prosecution

• *Gordon Hughes*

Australia's first prosecution of a person accused of spreading a computer virus ended in the Victorian County Court on 7 February 1991. The case of *Lynn v. Barylak* did not end as the authorities had planned. The defendant was acquitted and costs were awarded against the police.

The Facts

The defendant, Deon Barylak, was a mature age post-graduate student at Swinburne Institute of Technology in Melbourne. A qualified accountant, he had decided to take a year off work in 1989 in order to complete a diploma in business information technology.

As an enrolled student, Barylak had access to a computer laboratory which housed a network of Olivetti M24 twin drive personal computers.

At the time Barylak enrolled, the network was experiencing intermittent aberrant behaviour. Students were complaining that data was being inexplicably wiped off disks. It seemed that in certain circumstances, a command to format a disk in drive A could in fact cause the disk in drive B to be formatted, with the effect that data on the disk in drive B would be erased. It was subsequently determined that this aberrant behaviour was the result of a virus which could be implanted by use of a boot diskette. The virus would then reside in the RAM of the computer concerned and would disappear when the affected computer was turned off.

Until the cause of the problem had been isolated, it had been the Institute's practice to leave individual boot diskettes in drive A of each machine for students to use at will. Because this obviously facilitated the substitution of unauthorised diskettes containing the virus, this practice was changed when the source of the virus had been identified. In order to use boot diskettes, students were required to collect the diskettes from senior students and return them once their session was complete. Notices were strategically placed to publicise the new procedure, and students were also encouraged to turn off machines once they had finished using them.

The obvious intention of the new procedure was to ensure that only "clean" diskettes were used to boot the machines on the network. Nevertheless, the virus continued to appear. This meant that at least one unauthorised boot diskette was still in circulation and it was clearly necessary to identify the person who was using it.

Suspicion fell on the defendant. On 10 May 1989 he was observed by a senior lecturer using four terminals in rapid succession. He was observed sitting at each for about five minutes, booting up and then moving on, leaving each machine turned on. It was apparent he was using a non-standard diskette. When one of the machines was checked after the defendant left it, it demonstrated the presence of the virus.

The Institute's suspicions were reported to the police. The police raided the defendant's home and seized a non-standard boot diskette. The defendant said he had copied the diskette from another student and he admitted having used the diskette to boot up computers on the network in contravention of the newly published procedure. He told the police that many students use their own diskettes for reasons of convenience. He denied emphatically that he had been involved in spreading the virus.

Two charges were laid against Barylak. He was charged with "computer trespass" under the *Summary Offences Act* and with attempted criminal damage to property under the *Crimes Act*. The essence of the "computer trespass" charge was that he had gained "unauthorised access to a computer system." The essence of the attempted malicious damage charge was that, by implanting the virus and leaving the individual terminals switched on, the defendants had attempted to damage a diskette which might be inserted by a subsequent user.

The Law

Section 9A of the *Summary Offences Act* was enacted in 1988. The section provides 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." There has been one previously reported conviction under the section but no reported judicial interpretation of the wording.

With respect to the charges of attempted malicious damage to property, the *Crimes Act* s.197 provides that the offence occurs when a person "intentionally and without lawful excuse destroys or damages any property belonging to another." Under s.196, it is necessary for the "property" affected to be tangible in nature.

The requirement of tangibility has long been identified by academics as a potential stumbling block in a case of this nature. It would seem that in the event of data being erased from a diskette, there would be a lack of identifiable "damage" to the tangible property. Certainly there would be damage to the data itself but data, of course, is not tangible.

Two overseas cases had, nevertheless, previously addressed the issue in a matter favourable to the prosecution.

In the English decision of *Cox v. Riley* (1986), a conviction under the *Criminal Damage Act* was recorded against a defendant who deliberately erased a computer program from the plastic circuit card on a computerised saw. Although the defence argued there had been no damage to the tangible circuit card, the court ruled that the elements of the offence were satisfied where restoration of the tangible property to its original state would necessitate some work and some expenditure of money.

In the Canadian case of *Re Turner* (1984), a similar charge was brought against a defendant who had gained unauthorised access to a business competitor's computer tapes and encrypted the information in such a way that access to the data became impossible without knowledge of the new code. It was held that the crime had been committed, notwithstanding the absence of identifiable damage to tangible property, because "interference with the enjoyment of the property is the gist of the offence."

Legal Arguments

The defence failed in its submission that - regardless of the facts - the laws under which Barylak had been charged were inappropriate and incapable of sustaining a conviction.

In relation to the "computer trespass"charge under the *Summary Offences Act*, it was argued that the defendant did not, in fact, lack "lawful authority" to access the system. He was an enrolled student and authorised to be on the premises. As a business information technology student, he was authorised to use the computer laboratory and the individual terminals on the network in question. There had been a flouting of procedural requirements to the extent that the defendant used an alternative procedure to start the machines - but in isolation this should not deprive him of his "authorised" status.

At this point, concessions were made to the court by each side. The defence conceded that if it could be proved on the facts that the defendant had accessed the system for the illicit purpose of attempting to spread the virus, a conviction for computer trespass would necessarily follow - whatever authority he had to use the system, it did not extend to access for that type of activity. On the other hand, the prosecution conceded that if it were held that the defendant had not been attempting to spread a virus, then likewise the computer trespass charge could not be sustained - a breach of "in-house rules" did not deprive a person of lawful authority to access the computers.

Ultimately, it was held that the prosecution had failed to prove Barylak had acted with devious intent and, accordingly, the computer trespass charge was dismissed. Judge Byrne ruled that the offence, as pleaded by the informant, "involves the purpose on the part of the [accused] to do the mischief contemplated" and as there was insufficient evidence as to the defendant's intent, the charge was dismissed.

With respect to the charge of attempted criminal damage to property, the prosecution asserted that not only was the functionality of the diskette affected if data were erased, but also there was indeed a perceptible physical change to tangible property. When asked whether there was any physical change in a diskette before and after suffering the effects of a virus as described in this

case, prosecution witnesses Sen. Const. Maurice Lyon stated:

> *"Yes ... there is a very significant difference. That is, information is stored on the magnetic media by means of magnetic pulses or magnetic motor force. That is, the magnetism on the disk points one way or the other so the information is stored as a series of either magnetism one way or the other. Once the disk is formatted that magnetism has changed, or when you write to the disk that magnetism is changed so it is physically different to what it was prior to the command."*

Asked whether this physical difference was demonstrable in any way, Sen. Const. Lynn replied:

> *"Yes, it is. It is directly viewable on the screen using the appropriate software or meter if you like to determine what is on the disk surface."*

This contention was rejected by the defence. It was submitted that "tangible property", and hence damage to the property, had to be perceptible to the human senses. Barylak's counsel stated:

> *"Here the change is very subtle. It does not affect the value of the diskette. It affects the usability of the data on it. The data certainly is intangible. So damage could only have been caused here if you regard damage as the subtle alteration to the magnetic impulses, not something which can be seen easily but something to be measured through sophisticated equipment. Even then by running [a diagnostic test] you are not actually seeing it: you are seeing a reflection of the result."*

The Judge ruled in favour of the prosecution on this point. The concept of "tangible property" should not be restricted to the gross physical entity that can be perceived by the human senses but should also extend to all the characteristics of the physical property including, in this instance, its electrical characteristics.

It followed that, if the prosecution could prove that the defendant had in fact planted the virus as alleged, it would be open to the court to hold that he had been attempting to damage the diskette which a subsequent user might insert in the machine in question. It would be necessary to prove perceptible physical damage, but this could be satisfied by an alteration of physical properties detectable only through highly sophisticated diagnostic programs.

Factual Argument

The prosecution case was based on circumstantial evidence, as there was no direct evidence that the defendant had committed the offences the prosecution had to do more than prove that the accused's behaviour was consistent with spreading a virus. It had to prove that there was no alternative, reasonable explanation of the defendant's behaviour which might also be consistent with some other innocent activity.

In this regard, the defence elicited concessions from prosecution witnesses as to a number of alternative explanations of what had occurred on 10 May, 1989. One option was clearly a strong possibility - that Barylak had inadvertantly acquired an infected diskette when he copied the boot diskette from another student. This was a logical explanation which had not been the subject of any questioning by the police when they had raided the defendant's house and which had not been considered by the Institute's staff when the defendant had been confronted at the scene.

But what about the defendant's behaviour in moving from machine to machine in rapid succession, leaving the terminals switched on in the process?

Again, a logical explanation had emerged in the evidence of several witnesses. There had been numerous concessions that the machines were often faulty and that it was common for students to roam in search of a terminal or keyboard in working order. There was also evidence that it was common for students to leave machines on after use. As one prosecution witness had conceded:

> *"The new policy was that machines were supposed to be left off but because it took a while to get boot disks and because it is bad for a computer to turn it off and on because you cause power surges through the circuitry a lot of people left the computers on."*

The Ruling

On the basis that there were innocent explanations of the defendant's behaviour, the case was dismissed. Costs were awarded against the informant.

In forming his conclusion, the Judge emphasised the lack of evidence as to a motive on the part of the defendant.

Being a County Court judgement, the case is in one sense of limited jurisprudential significance. It is likely to have a profound impact, however, on the way in which police investigations proceed in future.

First, there must arguably be evidence of illicit intent in order to sustain a conviction for "computer trespass." Furthermore, it seems a breach of "in-house" regulations may not be sufficient to sustain a charge under that provision.

Secondly, the long-held theory that erasure or alteration of data stored on a diskette does not constitute damage to tangible property has again been brought into question.

Finally, an uncommon thoroughness will be required in police investigations of similar offences in future. When circumstantial evidence is to be relied upon (and this will generally be the case), it will be necessary to fully investigate the practical and technical feasibility of alternative explanations for aberrant behaviour in the system - even if such explanations seem to be improbable. It will be necessary, also, to produce evidence of a likely motive on the part of the accused.

In summary, the case is something of a landmark in an area of computer law largely devoid of judicial pronouncements in Australia. Perhaps it emphasises, if nothing else, that Victoria's computer crime laws are indeed vague and require urgent reassessment. It should be made clear, for example, whether motive is intended to be a component of the "computer trespass" offence, and it should not be necessary, in this day and age, to be arguing about whether erasure of data amounts to "criminal damage" under an antiquated statutory definition - greater specificity would assist all concerned. ■

Gordon Hughes LL.M Ph.D is a Partner, Lander & Rogers, Solicitors, Melbourne and President of the Victorian Society for Computers and the Law.

This article has been reprinted with permisston of the Australian Accountant.