# Some Aspects of Theft of Computer Software

by

M. Dunning

## I. INTRODUCTION

The purpose of this paper is to test the capability of New Zealand law to adequately deal with the impact that computers have on current notions of crimes relating to property. Has the criminal law kept pace with technology and continued to protect property interests or is our law flexible enough to be applied to new situations anyway? The increase of the moneyless society may mean a decrease in money motivated crimes of violence such as robbery, and an increase in white collar crime. Every aspect of life is being computerised—even our personality is on character files, with the attendant possibility of criminal breach of privacy. The problems confronted in this area are mostly definitional. While it may be easy to recognise morally opprobrious conduct, the object of such conduct may not be so easily categorised as criminal. A factor of this is a general lack of understanding of the computer process, so this would seem an appropriate place to begin the inquiry.

## II. THE COMPUTER

Whiteside[1] identifies five key elements in a computer system.

(1) Translation of data into a form readable by the computer, called input; and subject to manipulation by the introduction of false data. Remote terminals can be situated anywhere outside the central processing unit (CPU), connected by (usually) telephone wires over which data may be transmitted, e.g. New Zealand banks online to Databank. Outside users are given a site code number (identifying them) and an access code number (enabling entry to the CPU) which "plug" their remote terminal in. The numbers can be easily discovered (in one case they were posted on the walls

[1] Whiteside, *Computer Capers* (1978 Crowell).

of the computer room),[2] and "wiretapping" is the common crime in this area in America.

(2) Programing, which supplies the logical sequence of instructions for the solution of problems and dictates the manner in which the computer responds. Programs (an element of "software") can be stolen by remote terminal without anything being taken, but it is more than just copying. This paper is directed to the issue of whether or not the form a program takes in the computer and in its transmission (configuration of electrical charges, or electronic impulses) constitutes property as we define it in our criminal law.

(3) The CPU, commonly regarded as the "computer". Very basically this is a huge electronic binary abacus, pre-set by an operating system program to perform the necessary functions asked of it by user-programing. Its complexity creates problems for Fraud Squad detectives in detection of a fraud, but once detected, there are no problems in bringing the fraudsman to justice.[3]

(4) Output: translation of processed data into an intelligible form. Is it property while still a series of electronic impulses?

(5) Communication of output, also susceptible of wiretapping.

The property with which this paper is concerned is "software": whether in fact it is property that can be stolen. The best description can be found in *Honeywell, Inc.* v. *Lithonia Lighting, Inc.*,[4] which states that:

> Perhaps the best recognised and most easily understood dichotomy in the trade is between "hardware" on the one hand and "software" on the other, and even here the experts do not always agree as to whether a particular item falls in one category or the other. Generally speaking, "hardware" refers to the naked tangible parts of the machinery itself, while "software" denotes the information loaded into the machine and the directions given to the machine (usually by card or teleprompter) as to what it is to do and upon what command. "Software" is also frequently used to include "support"—that is, advice, assistance, counselling, and sometimes even expert engineering help furnished by the vendor in loading the machine for a certain program such as inventory control or preparation of payroll.

A computer system represents a large capital investment, and to be

[2] *Ward* v. *Superior Court of California,* 3 C.L.S.R. 206 (Cal., 1972); described by Parker, *Crime by Computer* (1976 C. Scribner's Sons), Chapter 11.

[3] This is based on discussions with Detective Senior Sergeant Doone of the Auckland CIB Company Fraud Squad. "In practice the problem is much more likely to be one of detection than one of finding a suitable crime to charge when it is detected": Tapper, *Computer Law* (1978 Longman), 117.

[4] 317 F. Supp 406, 408 (N.D. Ga. 1970). One can sympathise with the judge in this case, who earlier had said: "After hearing the evidence in this case the first finding the court is constrained to make is that, in the computer age, lawyers and courts need no longer feel ashamed or even sensitive about the charge, often made, that they confused the issue by resort to legal jargon, law Latin or Norman French. By comparison, the misnomers and industrial shorthand of the computer world make the most esoteric legal writing seem as clear and lucid as the Ten Commandments or the Gettysburg Address; and to add to this Babel, the experts in the computer field, while using exactly the same words, uniformly disagree as to precisely what they mean" at 408.

realised profitably, it must be utilised as continuously as possible.[5]

> Modern computers process information at a much faster rate than current technology allows such information to be supplied. As a result, time sharing systems are used: remote users send direct input data into the computer often simultaneously. After the data is received by the computer, it awaits processing for a brief period of time while the computer processes information of a higher priority. The computer proceeds down the hierarchical scale established by the operating system until each user's input data has been processed. As current processing units are capable of processing sometimes in less than a billionth of a second (nanosecond = 1,000,000,000th of a second) the varying users of the system experience little or no delay in receiving processed information and get the impression of a one to one communication with the computer. The time taken by the respective users in typing in the input from their remote terminals is used by the computer for the processing of other data, so that each new request is readily taken care of. Even with time sharing, the computer is often "on idle", the processing unit not analysing information because it isn't being supplied with the raw data with sufficient speed or in sufficient quantity. Although the idling time may be of a very limited duration, perhaps a second or two, the computer's capacity to process information is so great that it represents a rather significant waste of the computer's resources. Time sharing was developed in the first place to reduce the idling time of computers because it was very expensive to run when it wasn't actually doing anything.

Unauthorised running of data in this free time is another form of computer abuse that possibly is not proscribed by the criminal law.[6]

The tangibility of software "property" has meant a court sometimes having to find a tangible thing that was stolen, to which value was lent by the intangible. In one American case,[7] a point arose as to whether the accused had committed the offence with which he was charged since the article stolen had to be worth more than a threshold value of $50 to bring the statute into play, and the cards representing the program he had stolen were only worth $35. The victim company was allowed to adduce evidence to show that what the program would have commanded on the market for them was $5,000,000 and it was upon this value that the accused was convicted. However it may be that an unauthorised user may memorise something gained from a computer and later transcribe it into his own materials, thereby avoiding the sanction of this decision.

"The term computer assisted crime is used to designate any criminal activity where Data Processing (DP) equipment is used to perpetrate or facilitate an offence."[8] Two categories can be distinguished:

(1) the computer as an object of the crime;

(2) the computer as a tool of the crime.

In the first category no real problems are posed insofar as the property which is the object of abuse is tangible. Legislation against vandalism,

[5] Roddy, "The Federal Computer Systems Protection Act", (1980) 7 Rutg. J. Comp. L., 343, 35.

[6] Adams, *Criminal Law and Practice in New Zealand* (1971, Sweet and Maxwell), para. 1684.

[7] *Hancock* v. *State* 402 S.W. 2d 906 (Tex., 1966); affd. 379 F. 2d 552 (CA5, 1967).

[8] Francine McNiff, *Current Legislation Related to Computer Crime,* (1978) Caulfield Institute of Technology—Computer Abuse Research Bureau: Papers from a one day seminar, Dec. 6, 1978, p.83.

wilful damage, arson and the like is no less effective here than in any other context. However, damage to and theft of software depend upon the relevant definition of property to determine the efficacy of any charges brought.

The second category seems to have raised the most concern that the law is inadequate. The main reason for this belief is probably that most of the experience in this area stems from America, where their diverse and technically complex legal system has appeared at times to be tongue-tied in proscribing this sort of conduct.[9] While our criminal code provides a more encompassing and coherent system, definitional problems with regard to time, services, and software may still remain, and it is pertinent to examine the handling of these problems in other jurisdictions.

## III. The American Jurisdiction

In the words of one writer in this field,[10] "judges have been backed into juristic corners and have had to resort to cut and paste construction of wire fraud, grand theft and forgery statutes to bring various actions within the purview of some criminal statute."[11] Many states have enacted special criminal statutes to provide protection against theft of trade secrets, a term which can, in a broader definition of property, cover all the intangible assets of a computer. The problem with the common law basis of theft provisions is that it depends heavily upon the proprietary nature of those things within its ambit.[12] And in America it has been seriously doubted whether trade secrets have their basis in property.[13] Can one "steal" an electronic impulse? "The word 'steal' is a term of art, and includes the criminal taking of personal property with intent to deprive the owner permanently of the use of it": *Commonwealth* v. *Engleman*.[14] At common law, theft is

[9] Idem.

[10] Roddy, *op. cit.*, 352.

[11] Roddy, *op. cit.*, further the non-desirability of judges stretching a penal law to fit the circumstances, partly because "a person potentially subject to a criminal law . . . is entitled to a non-elastic reading of law to properly forewarn him that the conduct is sanctioned", and partly because "extension of the scope of the law by the courts to bring certain activities not foreseen by the draftsman within its scope, may encroach on the legislative function, a boundary judges strive not to cross". 352 (see note 74 post).

[12] Tapper, *Computer Law* (1978 Longman), 100.

[13] "[T]he word 'property' as applied to trade-marks and trade secrets is an unanalyzed expression of certain secondary consequences of the primary fact that the law makes some rudimentary requirements of good faith. Whether the plaintiffs have any valuable secret or not the defendant knows the facts, whatever they are, through a special confidence that he accepted. The property may be denied but the confidence cannot be. Therefore the starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs, or one of them.": Justice Oliver Wendell Holmes in *E.I. Du Pont de Nemours Powder Co.* v. *Masland* 244 U.S. 100, 102 (1917).

[14] 142 N.E. 2d 406 (1957).

predicted by the asportation of tangible objects, and the taking must be permanent. Hence the problem in the many American states that retain larceny provisions, of applying them to abuse of "software". There seem to be three requirements to satisfy a charge of larceny:

1) the property involved must be tangible personal property;
2) it must be asported;
3) there must be an intent to deprive the owner of it permanently. Electronic impulses do not move, per se, they merely trigger other impulses down a chain, and copying does not require movement of the copied article, as is put by one author Bequai,

> Larceny necessarily involves trespass to personal property whatever its form, and such property must possess characteristics which enable it to be "taken and carried away"; although it may be presentative of property of more substantial nature, it must possess some body of its own.[15]

Intangibles are only larcenable so long as they are rendered in tangible form, but Bequai goes on to say that intangibles are sometimes accepted to be within the realms of larceny, quoting the statutes making it an offence to secure a train ride without paying.[16] However these are exceptions only because of the special statutes involved. In normal cases of larceny for the offence to be committed it is required that the thing taken be tangible and have at least a nominal economic value. Once committed, the measurement of the value of the object taken (including that lent to it by its intangible element) will determine the seriousness of the felony.[17] For this reason it is argued in some quarters that because of this method of valuing the article stolen, larceny provisions are sufficiently effective in this area. But this view fails to recognise that such provisions do not cover the situation where the stolen "software" is not manifested in a physical form, but merely stored in the memory of the intruder's computer or copied onto his own material.

From the valuation theory it is an easy step to define theft of property in terms of deprivation of benefit to its owner. In *United States* v. *Lester,*[18] copies of valuable geophysical maps were made. The appellant (defendant) claimed that copies were not stolen property, but the court held that the property stolen was the valuable idea, not the paper embodiment. The earlier case of *United States* v. *Handler* stated that stolen property need not be taken larcenously, i.e. asportation and tangibility were not required and that 18 USC section

[15] *Latham* v. *State* 320 So. 2d 747 (1975).
[16] Bequai, *Computer Crime* (1978 Lexington Books), 29.
[17] *Hancock* v. *State* 402 S.W. 2d 906; *U.S.* v. *Lester* 282 F. 2d 750 (1960) (writings lent value to their media—geophysical maps); *U.S.* v. *Boltone* 365 F. 2d 389 (1966) (plans copied on own paper, but still value attached to object as containing 'ideas'); Susan H. Nycum, *The Criminal Law Aspects of Computer Abuse: Part I: State Penal Laws* 5 Rutg. J. Comp. L. 271 (1976) *People* v. *Dolbeer* 214 Cal. App. 2d 619 (1963) (theft of physical piece of paper on which list inscribed).
[18] 282 F. 2d 750 (1960).

2314 (the Federal statute in question) "is applicable to any [property] taken whereby a person dishonestly obtains goods or securities belonging to another with the intent to deprive the owner of the rights and benefits of ownership."[19] The use of the words "goods and securities" is perhaps unfortunate in light of the first statement that the property need not be tangible.

*Hancock* v. *State*[20] is the first major case to deal with computer abuse. An employee programmer of Texas Instruments Incorporation made photocopies of fifty-nine computer programs and attempted to sell them to one of his employer's customers for $5,000,000. The defendant contended that the programs did not constitute corporal personal property and therefore could not be the subject of theft. The court dismissed this argument because the section of the penal code with which he was charged specifically included within the definition of property "all writings of every description provided such property possesses any ascertainable value."[21] The value of the paper on which the programs were written was $35, not enough to trigger the $50 threshold of the statute. However there was no reasonable doubt that they were worth more than that and the vice-president of the company testified to their true value on the basis of his estimate of the price a willing buyer would pay for them to a willing seller. This leaves a problem where there is no available market or the seller never contemplated selling. Furthermore it skirts the issue of whether "software" is property capable of being stolen for in this case it was tangible property taken: The employer's paper on which the programs were copied. The situation is still not covered where the program is transferred from the memory bank of the victim's computer to the memory bank of the unauthorised user's computer, or where it is memorised for later transcription elsewhere.

Since that case, many states enacted trade secrets legislation, but it was not always effective. The major case was *Ward* v. *Superior Court of California*[22] involving two competing computer service companies, UCC and ISD. ISD had a valuable program that UCC would have liked to have obtained. They had a common customer which insisted on having the same site code number and billing number for both the companies' computers whose services it used. The access code number was easily obtained: It was posted in the computer room of ISD to remind its programmers. Ward, an employee of UCC, then simply telephoned into ISD's computer from the remote terminal at his office

[19] 142 F. 2d 351, at 353 (2d Cir. 1944).
[20] 402 S.W. 2d 906 (Tex., 1966).
[21] Tex. Penal Code Ann. tit. 7 s31.01.
[22] 3 C.L.S.R. 206. Parker describes the progress of this case in detail in *Crime by Computer*, (1976), Chapter 11.

and secured transmission of the programs to his computer's memory. He then had the program printed out, and took it into another office (which proved to be his undoing because it provided the transportation required under the statute with which he was charged: Section 499c of the California Penal Code—theft of a trade secret).[23] The definition of "article" under section 499c(a)1 is "any object, material, device or substance or copy thereof, including any writing, record, recording, drawing, sample, specimen, prototype, model, photograph, micro-organism, blueprint or map". It was held that only the copying of the program was a violation of the law (under section 499c(b)3)[24] and that the stolen electronic impulses had to be rendered into tangible form to bring the act within the scope of the statute. The definition of "article", the court considered, implicitly described only tangible objects "even though the [program] which the article represents may itself be intangible".[25]

Whiteside[26] suggests that had Ward used only visual readout instead of causing the program to be printed, there would have been no violation of California law. The District Court in *United States* v. *Seidlitz* found also that transmission of intangible electronic impulses is not theft of property, but the Court of Appeal (4th Circuit),[27] while affirming the lower court decision, thought that the WYLBUR system software, the subject of the offence, was property and it based this on the fact that:[28]

> OSI (Optimum Systems, Inc., the victim company) invested substantial sums to modify the system to suit its peculiar needs, that OSI enjoyed a multi-million dollar competitive advantage because of WYLBUR, and that OSI took steps to prevent persons other than clients and employees from using the system permit(s) a finding that the pilfered data was the property of OSI.

This seems to accord with the deprivation of benefit theory as a basis of theft and may neatly sidestep the issue of whether what can be stolen need be tangible, so long as it has a value to someone.

It may be that though the intangible need be rendered tangible to be stolen in America, the fact that it is manifested on material belonging to the thief will not avoid prosecution, so long as it is in fact rendered physical in some form. This is because of the case of *United States* v. *Bottone*,[29] where secrets were copies on the thief's own paper using his

[23] The relevant parts are:
Every person is guilty of theft who, with intent to deprive or withhold from the owner thereof the control of a trade secret . . . does any of the following:
(1) Steals, takes, or carries away any article representing a trade secret.
(2) Having unlawfully obtained access to the article, without authority makes, or causes to be made, a copy of any article representing a trade secret.
[24] Idem.
[25] 3 C.L.S.R. 206 at 208 (Super. Ct. Cal. 1972).
[26] Whiteside, *op. cit.*, 78.
[27] 589 F. 2d 152 (1978).
[28] *Ibid.*, at 160.
[29] 365 F. 2d 389 (1966).

own copier but it was held immaterial, so long as the secrets were put into *some* tangible form:[30]

> When the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owner should be deemed immaterial.

In a recent case, *United States* v. *Sampson*,[31] the defendants were charged with theft of computer time and in arguendo it was put to the court that "free" time (when the computer is "on idle") was not something that could be classified as property. Computer time and storage capacity, it was said, were more properly characterised as "mere philosophical concepts as distinguished from interests capable of being construed as property".[32] The court rejected this:[33]

> The consumption of its time and the utilization of its capacities seem to the court to be inseparable from the physical identity of the computer itself. That the computer is property cannot be questioned. This, the uses of the computer and the product of such uses would appear to the court to be a "thing of value" within the meaning of (18 USC) s641, sufficient upon which to predicate a legally sufficient indictment.

"The scope of state criminal laws protecting software is often determined by whether the software is property subject to protection."[34] Some American states, particularly the computer intensive ones (such as California, New York, Texas, New Jersey), have enacted trade secret legislation to protect computer software; others rely on larceny statutes containing broad definitions of property.

In the *Ward* case (ante), section 499(c) of the California Penal Code relating to theft of trade secrets was used. But as was shown, only the article representing the trade secret could be stolen: Judge Sparrow stated that electronic impulses ". . . are not tangible and hence do not constitute an 'article' capable of being stolen within California trade secrets law".[35]

A New Jersey law enacted in 1965[36] stated its purpose to be "to clarify and restate existing law with respect to crimes involving trade secrets and to make it clear that articles representing trade secrets, *including the trade secrets represented thereby,* constitute goods, chattels, materials and property and can be the subject of criminal acts" (emphasis added). The emphasised words seem to indicate that this statute avoids the pitfalls of the corresponding Californian provision, and that the intangible program itself can be the subject of theft, without it necessarily having to be manifested as an "article".

The Texas Trade Secrets Law[37] proscribes "stealing, copying, *com-*

[30] *Ibid.*, at 393.
[31] 6 C.L.S.R. 879 (N.D. Cal., 1978), noted by Roddy, (supra), at 355.
[32] *Ibid.*, 880.
[33] *Ibid.*
[34] Nycum, *ibid.*, at 272.
[35] 3 C.L.S.R. 206, 208 (Super Ct. Cal. 1972).
[36] N.J. Stat. Ann. s2A; 119-51.
[37] Tex. Stat. Ann., Penal Code s31.05 (1974).

*municating or transmitting* a trade secret without the effective consent of the owner of the secret"[38] (emphasis added). It would seem to be broad enough so as not to require asportation, and to cover intangible property as well (by making communication transmission an offence).

Larceny statutes are perhaps more relevant to the New Zealand situation containing, as they do, valuable definitions of property instructive to the New Zealand draftsman. New York uses a formula that is relatively common by defining property as "any article, substance of value".[39] This seems to subsume the decision in *People* v. *Dolbeer*[40] where lists of telephone subscribers were stolen and it was held that the list lent its value to the paper on which it was inscribed. This valuation rule had been applied in an earlier case within jurisdiction where it was held that the value of property stolen is what the thief would have had to pay to acquire the property.[41] Personal property is defined by New York statute to include intangibles as well as tangibles.[42] The leading case defining it in that jurisdiction is said to be *In re Bronson*[43] which states it to be "tangible property as well as intangible . . . that is capable of being owned or transferred".[44]

However, in the aforementioned state, theft of a trade secret is specifically included in the larceny law. Nycum[45] notes that four jurisdictions rely on codified or common law larceny alone and that little protection for software is afforded by them. This is because of the obvious difficulty of applying the basic elements of larceny, (mentioned earlier) to abstraction of software.

The "anything of value" formula is used in the lists of property subject to larceny in Delaware, District of Columbia and Florida, but Nycum doubts the efficacy of this to successfully encompass intangibles. With all due respect, it is submitted that it does. Once a phrase such as this is inserted in the definition of property in a statute, evidence can be adduced in a court as to the value of whatever is stolen, as was done in *Hancock* v. *State* (ante). Everything has a value, including intangibles such as time and services: If they did not, they would not be stolen (tape or paper programs would not be stolen were it not for their software value). This formula merely embodies the commonsense rules of the deprivation of benefit theory and provides the legislative intent necessary to enable a court to convict, and to

[38] Nycum, *ibid.*, at 278.
[39] N.Y. Penal Law, s155.35.
[40] 214 Cal. App. 2d 619; 29 Cal. Rptr. 573 (1963).
[41] *People* v. *Irrizari* 5 N.Y. 2d 142; 182 N.Y.S. 2d 361 (1959).
[42] Gen. Const. Law 39 (1967).
[43] 150 N.Y. 1; 44 N.E. 707, 711 (1896).
[44] But note the uncertainty made by the contrasting authority mentioned by Nycum, *ibid.*, at 280, n63.
[45] 5 Rutg. J. Comp. L. 284 (1976).

punish accordingly. Support for this is *United States* v. *Handler* (ante) where stolen property under Title 18 section 2314 of the U.S. Code did not have to be tangible, so long as the intent was to deprive the owner of the rights and benefits of ownership. Furthermore, the court in *United States* v. *Sampson* (ante), held computer time and services to be things of value within 18 USC 641, which uses the catch-all phrase, "anything of value" to define public property.

Generally speaking the American courts at both the Federal and State level have reflected the policy of the court in *Ward* (ante), and avoided the issue of whether an intangible such as software can be stolen, directing themselves instead to whether it has been expressed in a tangible form.

It is interesting to note the reception that value or control theories have experienced with regard to taxation of "personal" property (as opposed to real property) in America. The problem here has been in classifying software as tangible or intangible, the distinction being important in deciding what amount of tax is attracted. Two major cases must be mentioned. In *District of Columbia* v. *Universal Computer Associates*[46] it had to be decided whether the taxable value of a computer owned by the defendant company included its software (intangibles not being taxable). It was held that software is intangible and therefore is not liable to personal property tax. Compared with this is the case of *Greyhound Computer Corp.* v. *State Dept. of Assessments & Taxation*[47] which, on a similar fact situation, decided that software services were intangible but dicta indicated that information stored on a tangible medium would be considered tangible.[48] At another source[49] it was cogently argued that the content of software bears little relation to software media (tapes, printout, etc.), that it is important to identify them as two separate interests (cf. Nycum, ante), that the content lends value to its media and the tangible elements do not constitute the real value of the software. That this is so relies on basic commonsense; the problem is to base it in statute. Parker,[50] after describing an increasingly common transaction by electronic funds transfer (EFT) whereby wages are directly credited to an account and thence to other accounts in payment of bills (no physical negotiable assets changing hands) concluded that what goes on is a sort of balance sheet movement of assets evidenced by computer: "The pulses of electricity, patterns of magnetic areas on tapes, and

[46] 465 F. 2d 615 (1972).
[47] 271 Md. 674; 320 A. 2d 52 (1974).
[48] See Roddy, "The Federal Computer Systems Protection Act", (1980) 7 Rutg. J. Comp. L. 343 at 328, n109.
[49] Bryant and Mather, "Property Taxation on Computer Software, (Summer 1972) 18 New York Law Forum 59.
[50] Parker, *Crime by Computer* (1976 Scribner's Sons), 3-4.

disks (sic) and states of electronic circuits are the assets. They don't just represent assets in other forms, they are the assets!"

Opinion in America seems to be coming around to the belief that specific legislation is necessary to proscribe computer abuse. The enactment of various trade secret laws was a recognition of this, but they also seem to be ambiguous and inadequate. Consequently a bill was introduced at the federal level in 1977, called the Federal Computer Systems Protection Act, to enable heavy prison terms and stiff fines to be imposed on electronic burglars who use computer technology to steal or manipulate information and other property. " 'Property' includes, but is not limited to, financial instruments; information including electronically (processed or) produced data; and computer software and programs in either machine-or human-readable form, and any other tangible or intangible item of value".[51] Other definitions include Access, Computer, Computer System, Computer Network, Services, Computer Program and Computer Software. The Act will make it a felony, punishable by up to 15 years in prison, or a $50,000 fine, or both, for anyone who[52]:

> . . . directly or indirectly accesses or causes to be accessed any computer, computer system, computer network, part thereof which, in whole or in part, operates in interstate commerce or is owned by, under contract to, or operated for, on behalf of, or in conjunction with, any financial institution, the United States Government, or any branch . . . or agency thereof . . . for the purpose of (1) devising or executing any scheme or artifice to defraud, or (2) obtaining money, property, or services by means of false or fraudulent pretences, representations, or promises.

Bequai was involved in the drafting of this bill and says that it was intended to be as broad as possible to cover all types of computer crime. It is doubted whether such a drastic measure is needed in New Zealand, and the fact that the bill has yet to be passed in America suggests it probably is not required there either.

The Model Penal Code[53] is a more instructive source of provisions that might be used against computer abuse. "Property" is defined in section 223.0 as:

> Anything of value, including real estate, tangible and intangible personal property, contract rights, choses-in-action and other interests in or claims to wealth, admission or transportation tickets, captured or domestic animals, food and drink, electric or other power.

" 'Property of another' includes property in which any person other than the actor has an interest which the actor is not privileged to infringe. . . ." The offence of theft (consolidating the previous common law charges of larceny, embezzlement, false pretences, etc.) is constituted if a person (with regard to "movable property") "takes, or exercises unlawful control over, movable property of another with

[51] Krauss & MacGahan, *op. cit., Computer Fraud and Countermeasures* (1979 Prentice-Hall, Inc.), New Jersey, 313.
[52] Bequai, *op. cit.*, at 44 (see note 16 ante).
[53] American Law Institute (Philadelphia, 1962).

purpose to deprive him thereof" (section 223.2). " 'Moveable property' means property the location of which can be changed, including . . . documents although the rights represented thereby have no physical location". There is, unfortunately, no definition of "document". A definition such as can be found in section 263 of the Crimes Act 1961 (NZ), as inserted by 1973 Amendment No. 118, would be beneficial here to preclude an argument that "document" does not include magnetic discs and other high-technology media used by computers. For if theft requires "movable property" to be involved (section 223.2(1)), it may be argued that a document implies writings in an old-fashioned sense and therefore a program is not a document. But in rebuttal of this, it is submitted that because of the statutory construction that defines "including" as meaning "but not limited to", reference may be had to the definition of property in section 223.0(6) which includes intangible personal property. Furthermore, if section 223.2(1) is inadequate, recourse may be had to section 223.2(2): Theft of immoveable property. When an unauthorised user causes a computer to transmit a copy of a program, or data, he does not cause that thing which is entered in the victim's computer to be moved. It remains unchanged, just as if a photocopy is made of a page in a book: The writings still remain in that book. Hence, in many circumstances, software may be described as immovable property. On a physical plane, when something is caused to be transmitted by electricity, it is not really the thing itself that is transmitted. Rather, the electricity at the transmitting end is caused to be excited in a certain manner, which causes all the electrical charges down the wire to become excited, which in turn triggers the electrical charges at the receiving end to become excited in a certain way and convert into the desired output. Hence there is a good conceptual base for the argument that software (e.g. a program) is "immovable property" within section 223.2(2) by which "a person is guilty of theft if he unlawfully transfers . . . any interest (in immovable property) with purpose to benefit himself". However, if the computer invader takes completely the program from the victim's computer (erasing the victim computer's memory banks in the process), it would then, by logical definition, become "movable property" and section 223.2(1) could be brought into play.

It is pertinent to notice that the deprivation of benefit theory is used as a constituent of the offence of theft. "Deprive" means:

> (a) to withhold property of another permanently or for so extended a period as to appropriate a major portion of its economic value . . .
>
> Theft of services is specifically made an offence in section 223.7:
>
> (1) A person is guilty of theft if he obtains services which he knows are available only for compensation, by deception or . . . by false token or other means to avoid payment for the service. "Services" includes . . . professional service . . . use of vehicles or other movable property . . .

> (2) A person commits theft if, having control over the disposition of services of others, to which he is not entitled, he diverts such services to his own benefit or to the benefit of another not entitled thereto.

Although a computer is not "movable property" a program, as already argued, probably is and this provision is probably wide enough to be construed as covering the case where an unauthorised person accesses a computer to use its special functions, or merely to use its time.

The other relevant section of the Model Penal Code is 223.3: Theft by deception.

> A person is guilty of theft if he obtains property of another by deception. A person deceives if he purposely:
> (a) creates or reinforces a false impression. . . .

"Obtain" is defined in section 223.0(5) to mean:

> (a) in relation to property, to bring about a transfer or purported transfer of a legal interest in the property . . .; or (b) in relation to labour or service, to secure performance thereof.

Thus an intruder who uses another's site and access code numbers through a remote terminal is creating a false impression that he is who the code numbers say he is. And the victim would most certainly seem to have a legal interest in the software he possesses and controls. If this is put in doubt, the court may have recourse to the theft of service provision using the definition of "obtain" in section 223.0(5)(b). However a point has been raised in England with regard to obtaining services by deception, and that is that technically one cannot deceive a machine, only people.

## IV. The English Jurisdiction

The theory that property can be intangible is not alien to the common law. Choses in action have long been recognised as property interests, within which are included such ephemeral "things" as patents and copyrights:[54]

> For want of a better classification, these subjects (patents, copyrights, etc.) of personal property are now usually spoken of as choses in action. They are, in fact, personal property of an incorporeal nature. . . .

The Theft Act 1968 (U.K.) defines property in section 4(1) as including "money and all other property, real or personal, including things in action and other intangible property". Although seemingly wide, it has been held not to include information,[55] an unfortunate exclusion from the point of view of theft of information from a computer.

The Act has as its basic definition of theft in section 1 that:

> A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.

[54] Williams, *Personal Property* (1st ed. 1848 London), 6.
[55] *Oxford* v. *Moss* [1979] Cr. L.R. 119.

"Appropriates" means "any assumption by a person of the rights of an owner" (section 3), and "a person appropriating property belonging to another without meaning the other permanently to lose the thing itself is nevertheless to be regarded as having the intention of permanently depriving the other of it if his intention is to treat the thing as his own to dispose of regardless of the other's rights" (section 6).

Tapper[56] mentions that in debates on the Theft Act in the House of Lords, Lord Wilberforce expressly referred to "business secrets" as being within the scope of the definition of property. But it has been held that information is not.[57] It is submitted that the more problematical areas of computer abuse (theft of software, e.g. a program or data, via a remote terminal) are covered by these broad provisions. It is open to a court to find software to be intangible property that is stolen by copying, for by causing the transmission of data or a program, the unauthorised user is assuming the rights of its owner with an intention to treat the thing as his own to dispose of regardless of the other's rights. Halsbury's[58] comments that appropriation within its meaning in section 3(1) of the Act "replaces (the) requirement of pre-existing law of a trespassory 'taking' and 'carrying away' and although most instances of theft involve a taking of possession, the offence need not do so". Furthermore, "appropriation may also occur when a person not in possession of property assumes the rights of an owner even though he does not take or touch it at all".[59]

It would seem that it is recognised that what can be taken are the rights accruing to, and representing, property, without there being an actual taking of the property itself,[60] so to speak. The Act replaces and consolidates, inter alia, the common law offence of larceny, which relied on a permanent deprivation of a tangible and the new requirements indicate the modern trend to acceptance of the deprivation of benefit theory. Thus even though a program remains intact in a victim's computer after copying, some of the previously absolute ownership rights have been lost. Tapper considers that the section is not clear enough, depending ultimately upon how the property in question is conceived, and that the matter still being highly questionable requires explicit confrontation by statute.[61]

Another provision that seems to apply in this area, particularly to theft of services, has had its effectiveness challenged by at least two

[56] Tapper, "Computer Law" (1978), Longman, 106.
[57] *Ibid.*
[58] Halsbury's Laws of England (4th ed. 1978) Vol. 11, para. 1264, n1.
[59] *Ibid.*
[60] Property has been described, rightly so it is submitted, as a bundle of rights (see note 78 post).
[61] Tapper, *op. cit.*, 107.

writers.[62] Section 15 of the 1968 Act proscribes obtaining property by deception, but as Tettenborn validly points out,[63] one cannot deceive a machine. The same problem applies to section 1 of the Theft Act 1978 (U.K.) which replaces section 16(2)(a) of the 1968 Act with other provisions against fraudulent conduct, in particular obtaining services by deception. But in the case commonly used in this paper, remote access using another's code numbers is automatically allowed by the computer: It is not being deceived, but only operating within its functions. Only people can be "deceived" at law.

Resort may be had by the English prosecutor to other sections of the 1968 and 1978 Acts (but cut and paste sanctions are not desirable in the criminal law). For instance, section 13 of the 1968 Act (unlawfully using, wasting or diverting electricity) can be applied, (since electronic computers store and process information in the form of configurations of electrical charges), according to Tettenborn,[64] but not according to Tapper, since its ambit was "designed to catch the miscreant who either by-passed his own meter or tapped another's power supply".[65]

It has been held that falsification of potential computer input is within section 17 of the 1968 Act,[66] which proscribes, inter alia, altering a document or record required for any accounting purpose with a view to self-gain or loss to another. This relies on the accessed computer records being used for financial control (as opposed to stock control), and apart from which, (in New Zealand at least) defrauding a computer is really only a sophistication of accepted conceptions of the offence-fiddling manual books of account—and is legally uncontroversial.

It is submitted that given the definitions in sections 2 to 6 of the Theft Act 1968 (U.K.), especially that of "property" in section 4(1), the offence of theft as described in section 1 of the Act is sufficient to proscribe the conduct in the major American computer abuse cases mentioned. Theft of time and/or services would require the adoption of the robust interpretation used in *U.S.* v. *Sampson* (ante), or statutory intervention.

The definition of "property" and "theft" in the English act have been adopted by the Crimes Act 1958 of the State of Victoria (sections 71 and 72) as have the definitions of "appropriates" (section 73(4)), and "intention of permanently depriving" (section 73(12)). These provisions have been considered sufficient by one writer to "attach

[62] Tapper, *ibid.*, at 109; Tettenborn, *Some Legal Aspects of Computer Abuse* (1981) 2 Co. Law 147, 148.
[63] *Ibid.*, at 148, 149.
[64] *Ibid.*, at 149.
[65] Tapper, *op. cit.*, 109.
[66] *Att Gen's Reference (No. 1 of 1980)* [1980] 1 All E.R. 366.

criminal liability to activities such as destruction (theft) of a master file, software, components, etc. and, possibly, time".[67] It is doubtful whether time is covered, time not even being intangible property. It would have to be made a specific offence. The Victorian statute also adopts the deception provisions of the English act. Section 81 (corresponding with section 15 U.K.): Obtaining property by deception; section 82 (section 16 U.K.): Obtaining pecuniary advantage by deception; section 83 (section 17 U.K.): False accounting. The same writer believes these offences cover unauthorised use of time and services, but for the reasons already given in regard to the English provisions, it can be seen that they do not.

## V. New Zealand

"Property" is described in the Crimes Act 1961, section 2, as including "real and personal property, and any estate or interest in any real or personal property, . . . and anything in action, and any other right or interest. "The inclusion of "things in action" and "any other right or interest" and "personal property" comprehends some intangible property but probably not the sort with which this paper deals. The Act is a codification of common law and at common law intangibles were added to the list of property as the need arose (such as choses in action) rather than being a coherent concept of property in the abstract, comprising a collection of rights of "ownership" that can themselves be the subject of appropriation (as existed in Roman Law).

Section 217 describes "things capable of being stolen" as "every inanimate thing whatsoever . . . which is the property of any person, and either is or may be made movable" and theft under section 220 is:

> The act of fraudulently and without colour of right taking, or . . . converting to the use of any person, anything capable of being stolen, with intent:
> (a) To deprive the owner, . . . permanently of such thing or of such property or interest; . . .

This provision embodies the common law elements of larceny, especially in that asportation and an intent to deprive permanently are required to constitute the offence. Not only is software not larcenable (infra), it probably also is not a thing capable of being stolen within section 217 (and therefore, also, section 220). This is supported by the case of *R* v. *Bennitt*,[68] in which McGregor J in the Supreme Court said:

> What is capable of being stolen is defined . . . as every inanimate thing which either is or may be made movable. It seems to me under that definition that a thing capable

[67] Francine McNiff, "Current Legislation Related to Computer Crime" (1978) Caulfield Institute of Technology—Computer Abuse Research Bureau: Papers from a one day seminar, Dec. 6, 1978, at 83.
[68] [1961] N.Z.L.R. 452 at 454.

> of being stolen is something in the nature of a chattel which can be taken out of the possession of the owner.

He further said that "a bank credit or chose in action is therefore not capable of being stolen. It is not an inanimate thing but a right."

There is unfortunately no definition, as in the Theft Act 1968 (U.K.), of an intention to deprive permanently. Without the extended meaning given to it in that act, it can only be given the common law meaning of permanent deprivation of a tangible object. This also renders section 220 ineffective against the unauthorised computer user who causes to be displayed on his remote terminal, or to be printed out, any software in the victim's computer, since the subject-matter still remains in that computer.

Theft of electricity, section 218, suffers from the same defects as those mentioned with regard to the corresponding English provision (section 13, 1968).

The Crimes Amendment Act 1973 may be interpreted as going at least some of the way to proscribing computer abuse. "Document" was amended to mean, inter alia,[69]

> any disc, tape, wire, sound track, card, or other material or device in or on which information, sounds, or other data are recorded, stored or embodied so as to be capable, with or without the aid of some other equipment, of being reproduced therefrom; or . . . (e) any material derived, whether directly or by means of any equipment, from information recorded or stored or processed by any device used for recording or storing or processing information.

Unfortunately, possibly by legislative oversight, this definition applies only to sections 263 to 279 (the forgery sections), thereby making section 229A (introduced by the Amendment) practically ineffective here. Otherwise section 299A(b), using a document to obtain a pecuniary advantage, could have been useful. The provision is not aimed at computer abuse, per se, anyway. In the debates in Parliament on the amendment, its purpose was said to be to cover the situation where, for instance, a credit card was stolen having an intrinsic value of less than $10 and therefore attracting a maximum penalty of only three months imprisonment.

However, two other provisions dealing with documents were also introduced. The first, section 266A, makes it an offence for any who:

> With intent to defraud, —
> (b) By any means, makes a document that is a reproduction of the whole or any part or parts of another document.

This would seem to be applicable to the situation such as in *Ward* v. *Superior Court of California* (ante) where an intruder causes software to be transmitted. Whether the data is stored on magnetic tape, or is a program embodied in the electronic makeup of the computer, both are "documents"; and the receipt of the software at the intruder's end, be it by visual display, magnetic tape, punch cards, or printout, also

[69] s5(1)(c) & (e), 1973 No. 118.

constitutes a document.

One might perhaps contend that since a machine cannot be deceived, it cannot be defrauded either and therefore an intent to defraud a computer is negatived. It would be legalistic hair-splitting to argue that since an intent to defraud requires a person as its object, and a computer is not a person, then the offence under section 266A cannot be committed by abstraction of software. The person would obviously appear to be the "owner" of the software, or at least the owner of the hardware (the computer). Adams on Criminal Law and Practice in New Zealand[70] states that "intent to defraud may exist though no one was in fact defrauded". It is also "unnecessary that there should be any gain or benefit to the accused".[71] In the English case of *Feely*,[72] "fraudulently" or "dishonestly" was equated with moral obloquy, and the forgery case of *Welham*[73] removed the distinction between intent to defraud and intent to deceive, in that it had previously been thought that the former required proof of economic loss. Lord Radcliffe had this to say:[74]

> Now, I think that there are one or two things that can be said with confidence about the meaning of this word "defraud". It requires a person as its object: That is, defrauding involves doing something to someone. Although in the nature of things, it is almost invariably associated with the obtaining of an advantage for the person who commits the fraud, it is the effect upon the person who is the object of the fraud that ultimately determines its meaning.

*Miller*,[75] a New Zealand case, followed similar lines in not requiring proof of an ulterior motive or benefit to the accused.

Although the intent must be to defraud some person, nobody need suffer to make it criminal. The authorities seem only to require a dishonest intent in dealing with property, yet Lord Radcliffe's final words seem to comprehend the deprivation of benefit to some person against whom an act of moral obloquy is perpetrated. Section 266A(2) states that the offence is complete as soon as the act is done with this dishonest intent.

The actor in each of the American computer abuse cases mentioned, then, would be caught by this section. Even had the defendant Ward not copied down the program he caused to be transmitted, the display of it on his terminal would constitute making a document (assuming, of course, that it could be proved). It cannot be doubted that his intent, to steal a competitor's development, was dishonest. Really the mens rea elements of these particular offences is not a problem; the problem lies in whether the act is criminal.

[70] Para. 1884.
[71] Idem.
[72] [1973] 1 All E.R. 341.
[73] [1961] A.C. 103.
[74] At 123.
[75] [1955] N.Z.L.R. 1038, 1048.

Section 266B seems to be aimed at the third party who comes into control of a stolen document. To constitute the offence, the user must have knowledge that the document was "made in a manner, and with the intent referred to in subsection (1) of section 266A". The fraudsman who is caught under section 266A would also be caught under section 266B if he attempted to use the document he "made", but an innocent purchaser of it (or user of a computer bureau that implemented a stolen program) would not be. An independent offence of theft of computer time would not be necessary so long as a "document" was made, as the use is indivisible from the length of time for which the computer was utilised, constituting the one offence. However, these provisions do not cover the situation where the intruder, knowing a computer to operate with a certain program (as for instance the users of the Auckland University computer know the "languages" in which that computer operates) merely inputs from his terminal, or even on site, functions he wants performed, and receives a "solution" rather than a "document". In the case of a computer bureau, the user has clearly received something of value and hence deprived the bureau of value it could have received. It is not unlike using a rental car without paying, except in that case the offence of conversion proscribes the conduct.

Another criticism that can be levelled at the adequacy of these provisions to proscribe theft of software is that they come under the category of forgery in the Crimes Act and imply the use of computer software as an instrument of crime, rather than as an object in itself. In the debates in Parliament on the introduction of this bill, it was said to be primarily designed to close the gap of a Court of Appeal decision in 1971,[76] where sophisticated reproduction techniques were used to perpetrate a forgery (a photocopier). Sections 266A and 266B are similar in wording to sections 264 (forgery) and 266 (uttering forged documents). It may be that by a happy chance the new provisions can be applied to theft of software, but as already stressed, it is not desirable for the criminal law to be liberally stretched to fit all manner of conduct. Ambiguities obviously exist, to which statutory attention should be given.

## VI. Property Law: An Overview and Some Suggestions

Traditional property theory divides property into "real" or "personal", and property law, being concerned with the legal rights which enable individuals to protect or acquire wealth,[77] has developed with

[76] The case the Minister of Justice describes seems to be *R* v. *Tait*, but that is a 1968 case. New Zealand Parliamentary Debates, Vol. 382, 6 March, 1973; pp.494, 495.

[77] Bryant & Mather, "Property Taxation of Computer Software" (summer 1972) 18 N.Y.L.F. 59, 66.

society to vary emphasis as to which rights should be protected according to the importance placed on them by that society. The area of personal property (all that which is not real property) has had the greatest development: The class is indefinite but not unlimited. The law has been able to accept intangibles as personal property but not to any great extent. They lie within the category of choses in action, which include all rights and privileges which require to be enforced by an action in law or equity. Perhaps the closest English law has come to permitting of an abstraction describing property in terms of the rights it represents is in the field of land law, with the concept of seisin. It was recognised by Austin that ownership was constituted by a "bundle of rights".[78] Crossley Vaines on Personal Property says that English law has never had a theory of ownership, being "concerned only to settle dispute between two litigants and has had no action like the *vindicatio* of Roman Law to protect an abstract *dominium*".[79] Hence was it possible for Adams to state that "Roman Law treated theft of the use of a thing, or of its mere possession, as a form of theft (Steph., HCL iii 131-2). But it was never so at common law. . . . It is not theft to take without authority the temporary use of another's chattel"[80] (except insofar as proscribed by statute: e.g. the offence of conversion). Furthermore, Russell on Crime states[81] that "it has always been recognised that the temporary use of another man's property, although unauthorised by him, and wrongful, is not felonious: 1 Hale 509".

In Roman Law there existed the absolute right of *dominium* over *res,* which could be either *corporales* or *incorporales*—"The intangible thing or *res incorporales* is the right itself".[82] Burdick[83] states that the "things that were the subjects of property, or of ownership, were associated with rights in property", and Dias[84] perhaps recognised this when he stated that the term "ownership" "is a convenient method of denoting as an (sic) unit a multitude of claims", and that the right of ownership is distinct from its contents. Support for the deprivation of benefit theory as a basis of theft is given by his further statement that[85] "it is no doubt true that the exact value of a person's ownership will be affected by the extent of the advantages that he is able to derive. . . ."

[78] Crossley Vaines, *Personal Property* (5th ed. Butterworths 1973), 39.
[79] *Ibid.*
[80] Adams, *Criminal Law and Practice in New Zealand* (1971, Sweet and Maxwell), para. 1684.
[81] 12th ed. (1964 Stevens), at 999.
[82] Crossley Vaines, supra. 14.
[83] Burdick, *Principles of Roman Law and Their Relation to Modern Law,* Rochester, N.Y., Lawyers Co-operative Pub. Co. (1938) U.S.
[84] Dias, *Jurisprudence* (4th ed., 1976 Butterworths), 472.
[85] *Ibid.*, at 396.

It is fair to say that property in Roman Law included not only property in its ordinary sense, but also all rights in property. It is submitted that this is an element sadly missing from our modern conceptions of the word. Instead of concentrating on abuse of another's possession of a "thing", the law should proscribe the abuse of that person's ownership of it. Ownership has been defined by Pollock[86] as "the entirety of the powers of use and disposal allowed by the law". If property comprises a collection of rights and the criminal law is concerned to protect the rights of a member of society with regard to the other members, any law of theft must have as its basis the removal of one person's rights by another: It must become more effect-oriented.

Combined with the requirement of certainty and non-elasticity in the criminal law, the result is that some amendments may be necessary to the Crimes Act. The definition of "property" should be clarified by at least adding intangibles to it, along a similar vein to that to the Theft Act 1968 (U.K.). The best solution would be the adoption of an "anything of value" definition such as section 233.0(6) of the Model Penal Code (the *res* of Roman Law was whatever thing could be assessed in terms of money; have a cash value placed upon it).[87]

The main obstacle to applying the theft provisions to computer abuse of software is section 217, which should be amended to reflect a modern theory of property recognising rights in property as capable of being taken. Theft under section 220 should not be bound by the common law requirements of larceny, by either removing the need for asportation and permanent deprivation, or defining them widely such as in the English Act, so that the use of a thing may be stolen. If theft of the use of a computer cannot satisfactorily be proscribed that way, perhaps it can be done by adding to the list of things that can be converted in section 228, "any machine".[88]

## VII. Conclusion

While a criminal code is more desirable because of its simplicity than, say, the American legal system, there is a danger of over-codifying behaviour: One does not want to enact a new provision *every* time a new permutation of criminal behaviour arises. Ideally the elasticity of a common law system will supply the omissions of the

[86] Pollock, *First Book of Jurisprudence* (1904), Macmillan, 2nd ed.), at 179.
[87] J.A.C. Thomas, *Textbook of Roman Law* (1976 North Holland Pub. Co.), 125.
[88] "Conversion" may then become quite a useful provision. Adams (*ibid.*), para. 1686: "By treating fraudulent conversion as an alternative to fraudulent taking, s220 has not only rid us of most (if not all) of the problems arising from the adherence of the common law to the doctrine that the essence of theft was a wrongful interference with possession, but has also brought within reach of the criminal law many acts having all the iniquity of theft but formerly outside that law." See also para. 1727.

legislature but there are limits to which our judiciary will, and indeed can, go. It is suggested that in the area this paper covered, the minor amendments put forward are necessary to modernise provisions whose historical base has been eroded.