Computer Crime: The Law in '80

MICHAEL GEMIGNANI*

I. INTRODUCTION

Although various devices to speed numerical computations and the processing of data have existed for many centuries,[1] the electronic stored program, general purpose computer was not invented until the latter half of the 1940's.[2] The first computers were enormous, slow, and unwieldy devices compared to today's machines, dependent as they were upon bulky and inefficient vacuum tubes. The coming of transistors provided a major impetus to computer technology. Today, more efficient and exotic forms of "hardware" presage future computers that are smaller, faster and more powerful.[3]

There is scarcely anyone in the United States, no matter how poor or isolated, whose life is not touched significantly by computers. Now that there are rather powerful, general purpose computers which are sufficiently small, inexpensive, and easy to use to be practical for use at home,[4] and with electronic funds transfer looming on the horizon,[5] computers are certain to have an even greater impact on society in the future.

---

*Chairman of the Mathematical Sciences Department, Indiana University-Purdue University at Indianapolis (IUPUI); Acting Chairman of the Computer Sciences Section, Indiana University-Purdue University at Indianapolis. A.B., University of Rochester, 1962; M.S. & Ph.D., University of Notre Dame, 1964 & 1965; J.D., Indiana University School of Law-Indianapolis, 1980.

The author expresses his gratitude to Associate Professor Henry Karlson for many helpful discussions.

[1]Perhaps the earliest computational device, apart from fingers, is the abacus, which is fully 5000 years old. For a short history of computing machines, see 4 ENCYCLOPEDIA BRITANNICA 1046-47 (1974). Useful texts include A. CHANDOR, A DICTIONARY OF COMPUTERS (1970); READINGS FROM SCIENTIFIC AMERICAN, COMPUTERS & COMPUTATION (1971); F. SCHEID, INTRODUCTION TO COMPUTER SCIENCE (1970); A. TANENBAUM, STRUCTURED COMPUTER ORGANIZATION (1976).

[2]The Princeton mathematician John von Neumann is generally credited with the invention of the stored program computer. 4 ENCYCLOPEDIA BRITANNICA 1047.

[3]Innovations may cause legal problems. For example, computer abuse legislation may be framed in terms of "electronic computers," but many computers of the future may not be electronic at all. *See* text accompanying notes 133-35 *infra*.

[4]Complete computer systems, including a wide variety of accessories, are available for less than $2000, and the price is almost certain to fall. A basic home computing system can be purchased for less than $1000.

[5]*See* R. FREED, COMPUTERS AND LAW 634 (1976). *See, e.g.*, FLA. STAT. ANN. § 659.062 (West Supp. 1979); IOWA CODE ANN. § 524.803 (West Supp. 1979-80); ME. REV. STAT. tit. 9-B, §§ 131(14), (35), 334 (West Supp. 1979).

Computers have brought about a revolution in our century comparable to the industrial revolution of the previous century. Just as the industrial revolution necessitated a rethinking of much of the law of its time, so too the computer revolution poses legal questions today that must be addressed and answered. This Article will attempt to explore a limited number of those questions as well as some suggested answers. The emphasis herein will be on computer "abuse," and, in particular, "crimes" which present special problems under existing law.

A. General Forms of Abuse Involving Computers

Donn Parker of the Stanford Research Institute, probably the foremost expert today on the technical aspects of computer abuse, classifies forms of abuse involving computers under four headings:[6]

1) The computer itself is an *object* of attack or some abusive act, as, for example, firing a bullet into a computer or bombing a computer center.[7] This form of abuse can almost always be treated under the standard law governing crimes or torts against property and generally presents no substantially new legal issues.[8]

2) The computer creates a unique *environment* for the abuse or forms the source of a unique type of asset. For example, someone familiar with the operating system of a particular computer might attempt to erase valuable files in the computer's memory, or cause the system to "crash,"[9] often with major inconvenience and expense to the computer operator and the user of the machine. Yet another example of this form of abuse occurs when one business infiltrates the computer system of a competitor in order to steal trade secrets

---

[6]D. PARKER, CRIME BY COMPUTER 17-22 (1976). Parker summarized this classification in testimony before the Senate Subcommittee on Criminal Laws and Procedures in June 1978 when the subcommittee was considering S. 1766, the Federal Computer Systems Protection Act. *Federal Computer Systems Protection Act: Hearings on S. 1766 Before the Subcomm. on Crim. Laws & Proc. of the Senate Comm. on the Judiciary*, 95th Cong., 2d Sess. 56 (1978) (statement of Donn Parker) [hereinafter cited as *Hearings*].

[7]*See* D. PARKER, *supra* note 6, at 18 for accounts of four instances of assaults upon a computer with a gun. The most tragic episode, involving a bombing of a computer, resulted in the death of a graduate student at the University of Wisconsin. For an account of both this episode and the bombing of a Pentagon computer, see SENATE COMM. ON GOVERNMENT OPERATIONS, 94TH CONG., 2d SESS., PROBLEMS ASSOCIATED WITH COMPUTER TECHNOLOGY IN FEDERAL PROGRAMS & PRIVATE INDUSTRY 107 (Comm. Print 1976) [hereinafter cited as PROBLEMS].

[8]A fiction writer might come up with a plot involving a program which causes a computer to destroy itself. In actual practice, programs designed to cause trouble can only destroy, alter, or copy other data or programs, that is, they really affect software rather than hardware. This problem is discussed in the next section.

[9]*Hearings*, *supra* note 6, at 56.

or data which provide an edge in bidding on a contract. Abuses under this heading often present significant new legal questions.

3) The computer can be the *instrument* of the abuse. Crimes that might be classified under this heading range from murder perpetrated by causing a deliberate malfunction of a computer which governs a life support system[10] to the theft of computer time through the unauthorized use of a machine. Here again, novel legal issues may be presented.

4) A computer may be merely a *symbol* used in fraud, intimidation or other unsavory activity. Someone who falsely advertises that he is able to accurately predict the behavior of the stock market by means of a unique computer program, when he has no computer or computer program and is merely guessing what will happen, is indulging in this form of abuse. A collection agency which threatens a debtor by telling him that it will transmit his file from its computer to the computers of government agencies would be attempting to exploit the debtor's worst fears of what a computer can do. Despite the fact that the computer makes these practices possible, they do not generally raise significant new legal issues.[11] The computer is merely a tool of the tort or the crime.

B. The Computer

A computer is a machine which processes data.[12] What the computer does with data is determined by instructions given it by the user. Very simplistically, a computer may be thought of as a huge array of switches, each of which is either on or off. Some of the switches are set in accordance with the manufacturer's design of the computer. Other switches are set by the individual user according to the specific task he wants the computer to perform. The process of setting the switches is called "programming." Setting those switches which "bring the machine up" and prepare it to accept data and instructions from various users involves an "operating systems program." Once the machine is "up," a user then sets other switches to prepare the machine to do his particular job; generally, the user does this by means of an "applications program" written in one of the higher level computer languages such as FORTRAN or COBOL;

---

[10]Destruction of life can also occur through misapplication of air traffic control computers and computers governing military weapons. *Id.* at 59.

[11]If someone actually has a computer, but no valid means of predicting the behavior of the stock market, the usual rules of law concerning fraud, deceit, negligence, and breach of warranty, would apply.

[12]The definition of a computer is not so obvious. *See* notes 151-53 *infra* and accompanying text.

such a program is called a "source program."[13] The fully programmed computer may be thought of as a machine especially designed to take the data given it by the user and process that data according to the directions embodied in the applications program.

Even though the computer is a machine, it is quite different from virtually every other machine previously known to mankind. In the first place, the computer works at speeds which defy the imagination. Even an extremely slow computer can perform tens of thousands of computations in a single second. The speed of a computer provides its real utility; there is nothing that a computer can do that cannot be done manually given enough manpower and enough time. But the computer can compress man-years of work into minutes and digest libraries of information at virtually the speed of light.

A second important aspect of a computer is that each time it is used, it is, in effect, redesigned internally. The internal design, however, is often impossible to observe and difficult to check. Both the operating systems program and the source program for some particular job may be so complex that no human being could reasonably check the accuracy of each and every switch setting to be certain that the computer was properly prepared to do the task that the user set for it, even assuming that the programs themselves are logically correct and stated in a form that will lead the machine to produce the intended result. Furthermore, the switches of a computer are not like lightbulbs; one cannot tell if they are on or off by simply looking at them; indeed, most of them are too small to be seen with the naked eye.

Consider a black box within which is a small genie who will answer any question asked provided it is posed in exactly the right way. Someone who has a particularly difficult question tries very hard to phrase it in precisely the form that the genie will understand. The dilemma is compounded by the fact that the genie will always provide an answer when asked any question, even questions which are improperly worded. After a great deal of hard work, the questioner places his question in a slot at one end of the box and receives an answer from a slot at the other end. He receives the answer to his question if it was entered in exactly the right form; otherwise, what he receives is worthless. What credence should he place in the answer? This parable illustrates but one of the many problems associated with the use of computers.

---

[13]A source program is written in a high-level language such as FORTRAN (Formula Translation) or BASIC (Beginner's All-purpose Symbolic Instruction Code). This source program is translated inside the computer by means of a "compiler" into an object program written in machine language which actually sets the switches.

C. *Abuses Peculiar to Computers*

Some of the forms of abuse peculiar to computers are beginning to take shape. For example, the incredible speed coupled with the vast quantities of data processed can enable small crimes to pay rich dividends. One form of theft by computer is known as the "salami technique." This involves taking a small amount, like thin slices of a salami, from a large number of sources. The computer of a large bank may handle tens or hundreds of thousands of accounts.[14] The perpetrator of a theft employing the salami technique would arrange for the computer to transfer very small amounts of money from randomly selected accounts into an account which he controls. Only $.10 may be transferred in a given month from any one account, and the number of accounts affected at any one time would be but a fraction of the total accounts the bank services, but the overall amount of money siphoned off would be sizable.

Banks usually find it more convenient simply to credit an account alleged to be short $.10 if a customer complains; and, of course, most customers will simply assume that they made some error, write off the loss when reconciling their checkbooks, and never notify the bank at all. The small patch of program which effects the transfers will probably be skillfully concealed in an enormously large and complex program or made a part of the operating system of the computer, thus defying easy detection.

Because the perpetrator in this case would presumably have access to, and intimate knowledge of, the bank's computer system, he could destroy or modify the program as necessary if he found that a detailed audit was about to take place. In actual fact, however, the bank would almost certainly find it cheaper to just pay the small sums and not even conduct the time-consuming and expensive investigation needed to confirm that a theft was taking place. Note that the theft takes place at high speeds and totally automatically, untouched by human hands and unseen by human eyes. Such a scheme would be totally impractical, or at least much more risky and much less profitable, if the perpetrator had to transfer such amounts manually and personally keep all of the records in balance.

D. *Difficulties in Prosecution*

The blunt fact is that few prosecutions ever result from computer crime. Even the scope of the problem is not entirely clear. Donn Parker in his exhaustive study of computer abuses has found

---

[14]For an account of a theft using the salami technique, see *Hearings*, *supra* note 6, at 62-63.

only several hundred cases, and not all of these have been confirmed.[15] Many of the instances found by Professor Parker do not involve abuse integrally linked to the special characteristics of a computer.[16] Nevertheless, the average loss per instance of computer abuse, not counting the massive Equity Funding caper,[17] is $450,000,[18] more than five times the amount of the average loss sustained in 1971 from more traditional embezzlement schemes.[19] Obviously, any single computer-aided swindle can result in the loss of billions of dollars. Considering the prevalence of computers[20] and the apparent opportunities for improper gain, there are surprisingly few reported cases of computer crime. Many computer systems have significant crosschecks, audit trails, and other safeguards which serve to deter abuse, or at least make it more difficult, but even in cases where a thief has been caught red-handed, employers have often been unwilling, for various reasons, to prosecute. First, there is the embarrassment that an employer would suffer from publicly acknowledging that someone has cheated him and his customers using his own, supposedly reliable, computer. Second, many prosecutors and judges do not like to handle cases involving computers for the same reason that many students avoid mathematics courses: they simply do not understand them. For example, there is the problem of effecting a search of a computer even with a valid warrant.

---

[15]D. PARKER, *supra* note 6, at 23-40. For an extensive study of computer abuses within government, see PROBLEMS, *supra* note 7, at 76-117. A moderate litany of computer abuses is recited in J. CARROLL, COMPUTER SECURITY (1977). The number of reported cases involving computer abuse, however, is miniscule.

[16]Of the cases which Parker found, 37% fall under headings 1 and 4 which generally do not involve new questions of law. *See* note 6 *supra* and accompanying text. Of course only a fraction of the cases under the other headings will actually involve novel legal issues.

[17]*See* D. PARKER, *supra* note 6, at 118-74. Certain officers of Equity Funding created fictitious insurance policies and sold them at a discount to other insurers. They paid the premiums to the purchasers of the bogus policies from premiums on legitimate policies they held for Equity. The scheme collapsed when the income from real policies could not meet the increasing obligations generated by the bogus ones. There is some question whether this was really a computer crime, but there is no doubt that it would have been impossible without the capability of computers for processing large amounts of information.

[18]D. PARKER, *supra* note 6, at 28.

[19]*Id.* at 32.

[20]In 1977, the government had more than 10,000 computers in use. STAFF OF SENATE COMM. ON GOVERNMENT OPERATIONS, 95TH CONG., 1ST SESS., STAFF STUDY OF COMPUTER SECURITY IN FEDERAL PROGRAMS 6 (Comm. Print 1977) [hereinafter cited as SECURITY]. In 1977, there were some 500,000 computer systems made by American-based companies in use throughout the world; it is estimated that there will be some 1,100,000 such computers in use in 1981. Amicus curiae brief for CBEMA at 17-18, Parker v. Flook, 437 U.S. 584 (1978).

There is simply nothing that can be seen by observing the computer itself that would provide any evidence against an embezzler. The prosecutor would have to bring along a team of computer experts familiar with the machine who could "dump" the files and then interpret them.[21] Furthermore, the clever programmer who is stealing a fortune in nickels and dimes seems far less a danger to society than violent criminals. In some instances, computer criminals fired for dishonesty from one job go right into another position of even higher trust and responsibility. Others have been hired at large salaries as security consultants to help catch less clever crooks.[22]

The technology of computers is changing so rapidly that the fast and efficient machines of today will soon seem as unwieldy and slow as the machines of two decades ago seem today.[23] With more powerful machines come better opportunities for security, but also more exotic opportunities for abuse. Because human beings remain the architects of all phases of computer operations, at least in their initial phases, it is doubtful that a theftproof system can ever be devised. With the advent of electronic funds transfer and increased intercommunication among computers, the potential for theft on a truly majestic scale will be more of a temptation than many experts will be able to resist.

This Article will examine the legal weapons available for use against computer criminals, including a brief summary of existing state and federal law, a consideration of the few reported cases involving computer abuses, and a discussion of new and proposed legislation addressed specifically at computer abuse. The Article will conclude with a review of the situtation in Indiana, including a recent trial in Marion County involving a fascinating instance of computer crime, and a proposal for statutory revisions aimed at controlling computer crime.

---

[21]For an account of a case in which such a search was conducted, see D. PARKER, *supra* note 6, at 85-96. For a copy of the search warrant itself and the property receipt, see R. FREED, COMPUTERS & LAW 483-84 (5th ed. 1976) [hereinafter cited as FREED].

[22]The most notorious example in this regard is Jerry Schneider, who used Pacific Telephone and Telegraph Company's computer to rob it of equipment. The total take may have been in the millions. Jerry might never have been caught if he had not been turned in by a disgruntled employee. He served 40 days and paid a $500 fine. He had to repay the telephone company some $8500, but he is making more than $100,000 per year now as a security consultant. His story is told in D. PARKER, *supra* note 6, at 59-70.

[23]Semiconductor technology is progressing so rapidly that the cost of computation is decreasing by a factor of 10 every 5 years. Sugarman, *On Foiling Computer Crime*, INST. OF ELECTRICAL & ELECTRONIC ENGINEERS. SPECTRUM, Jul. 1979, at 31, 33.

II. Existing State and Federal Laws

A. Previous Surveys

At least two in-depth studies have been made concerning existing state laws that might be used to combat computer abuse. One of these reports was written by Ms. Susan Nycum as part of a study of Infonet[24] sponsored by the General Services Administration.[25] Ms. Nycum's legal analysis appears both in a Senate committee print[26] and, in a somewhat expanded form, in a law review article.[27] Though it deals with most forms of computer abuse, it surveys the legislation of only eleven "computer intensive" states.[28]

Mr. David Bender published an exhaustive study in 1970 concerning trade secret protection of software.[29] An updated, but less comprehensive, version of his important work appeared in 1977.[30] The entire field of computer law is changing quite rapidly so that any survey of legislation and case law concerning computers is likely to be at least partially obsolete by the time it appears.[31] For example, at least two states have already passed statutes dealing explicitly with computer-related crime,[32] but none of this specialized legislation is dealt with in either study. A further *caveat* that must be observed in dealing with state statutory and common law is that generalizations are often impossible, or at least somewhat risky, because each state has its own distinctive interpretation of what the law is within its borders.

---

[24]Infonet is the largest administrative data processing (ADP) firm supplying such services to the government. There was some concern for the security of the system because certain inmates at Leavenworth Prison had access to the system. The prisoners were working under a contract with the Internal Revenue Service.

[25]The report was done under the general direction of Donn Parker of the Stanford Research Institute. Ms. Nycum is a partner in a San Francisco law firm, a collaborator with Mr. Parker in studies involving law and computers, and one of the nation's foremost experts in computer law.

[26]Security, *supra* note 20, at 195.

[27]Nycum, *The Criminal Law Aspects of Computer Abuse: Part I: State Penal Laws*, 5 Rutgers J. of Computers & L. 271 (1976).

[28]California, Delaware, the District of Columbia, Florida, Illinois, Massachusetts, New Jersey, New York, Pennsylvania, Texas and Virginia. *Id.* at 271.

[29]Bender, *Trade Secret Protection of Software*, 38 Geo. Wash. L. Rev. 909 (1970).

[30]Bender, *Trade Secret Software Protection*, Computer L. Serv. § 4-4, Art. 2 (1977).

[31]By way of example, Indiana, which had no trade secret statute at the time Mr. Bender wrote his article, passed such a statute even before the article appeared in print. Ind. Code §§ 35-17-31-1 to -5 (1976, repealed 1977). Recently, Indiana repealed that statute in favor of one which includes trade secrets in a list of items which can constitute the *res* of larceny. *Id.* § 35-41-1-2 (Supp. 1979). Despite this legislative activity, Indiana seems to have no reported cases dealing with theft of trade secrets.

[32]Ariz. Rev. Stat. Ann. § 13-2316 (1979); Fla. Stat. Ann. §§ 815.01-.06 (1978).

Ms. Nycum has also prepared a complete survey of existing federal legislation that might be used to prosecute computer criminals.[33] As is the case with state legislation, only a handful of statutes have ever actually been used to prosecute anyone for a computer-related crime, so much of what can be done with these statutes remains conjectural. New federal legislation addressed specifically to computer crime has been introduced by Senator Abraham Ribicoff;[34] this proposed statute will be discussed later in this Article.

The use of federal penal statutes requires a basis for federal jurisdiction. Because this Article is focused on abusive acts rather than jurisdictional issues, this question will not be pursued herein, but it is, of course, something that must be considered in any potential prosecution.[35] In certain instances, state legislation is assimilated into the federal criminal code, thus permitting federal prosecutions which would have been questionable under the federal statutes alone.[36]

B. Theft

Traditional forms of offenses against tangible property can almost always be dealt with without difficulty under existing law, even if a computer is somehow involved in the offense. If someone fires a bullet into a computer or burns down a computer center, there are no special legal problems presented. Difficulties in coping with computer abuse arise because much of the property involved does not fit well into categories of property subject to abuse or theft; a program, for example, may exist only in the form of electric

---

[33]Nycum, *The Criminal Law Aspects of Computer Abuse, Part II: Federal Criminal Code*, 5 RUTGERS J. OF COMPUTERS & L. 297 (1976).

[34]The Federal Computer Systems Protection Act of 1979, S. 240, 96th Cong., 1st Sess., 125 CONG. REC. S645 (Jan. 25, 1979). The predecessor of S. 240 was S. 1766. *See* note 6 *supra*.

[35]*See* Nycum, *supra* note 33, at 298.

> The traditional method of defining federal criminal offenses not based upon . . . territorial jurisdiction or clearly devoted to the direct vindication of some weighty federal interest . . . has been to authorize federal punishment not for the familiar types of wrongdoing themselves but for the use of federal channels in connection with such wrongdoing.

Levine, *The Proposed New Federal Criminal Code: A Constitutional and Jurisdictional Analysis*, 39 BROOKLYN L. REV. 1, 9 (1972).

[36]18 U.S.C. § 13 (1976) extends state law into various territories located within a state but otherwise exclusively subject to federal jurisdiction. These areas of special jurisdiction are listed in 18 U.S.C. § 7 (1976). The most important area is the federal enclave, that is, land acquired by the federal government with the consent of the state legislature for use in certain federal areas of concern, such as the construction of a fort.

impulses or a magnetic pattern on a tape. Also, even when a program of substantial commercial value is misappropriated, the person from whom it is "stolen" almost always remains in possession of the original.[37] Indeed, the original program may not have been moved so much as a single inch while being illicitly copied. It may be duplicated exactly via electronic signals over a telephone line from one computer to another without altering the original program in any way, even while the original is actually running.

The principal reason someone might wish to steal a computer program is to save the time, trouble and expense of writing the program himself. Computer programs can, of course, be both long and complex;[38] they may take months, or even years, to write and "debug."[39] Because it is uncertain presently whether programs can be validly copyrighted or patented,[40] and because, even if they can be, these traditional forms of protection are not well suited to computer technology, the most effective source of protection for valuable software is statutory and common law trade secret protection.[41]

---

[37]By using "trapdoor" or "Trojan Horse" techniques, a skilled computer thief can even cause a proper use of a program to be the trigger for its illicit and automatic transfer to his own control. In addition to more prosaic methods of copying programs such as photography and various copy processes, there are more exotic methods such as using the electromagnetic waves generated by a computer to "tap" its contents. *See, e.g.*, Sugarman, *supra* note 23, at 32.

[38]For example, the SABRE program employed by American Airlines in making plane reservations contains more than one million instructions and cost more than $30 million to produce. Burck, *"On Line" In "Real Time,"* FORTUNE, Apr. 1964, at 145.

[39]"Debugging" is the process of removing errors from a draft program. A computer is very unforgiving of mistakes; one misspelled word or a single misplaced comma in a program may cause the program to fail (not run at all), or to give an incorrect result. Debugging may be more arduous than writing the program in the first place.

[40]Although the Copyright Office accepts computer programs for copyright under a general policy of accepting anything for registration that might be copyrightable, there is a serious question whether such a copyright would hold up if challenged. Even if it is valid, it is not clear what real protection it confers. Patents are even more problematic. For recent and fairly comprehensive treatments of this complex question, see Davis, *Computer Programs and Subject Matter Patentability*, 6 RUTGERS J. OF COMPUTERS & L. 1 (1977); Gemignani, *Legal Protection for Computer Software: The View from '79*, 7 RUTGERS J. OF COMPUTERS, TECHNOLOGY & L. 269 (1980); Bigelow, *Copyrighting Programs—1978*, [1978] 3 COMPUTER L. SERV. § 4-3 Art. 4; Ross, *The Patentability of Software and Firmware*, [1978] 3 COMPUTER L. SERV. § 4-2, Art. 5.

[41]In the 1960's, the fear arose that federal law had preempted state trade secret law. This fear was based upon Supreme Court decisions in Lear, Inc. v. Adkins, 395 U.S. 653 (1969); Compco Corp. v. Day-Brite Lighting, Inc., 376 U.S. 234 (1964); and Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225 (1964). More recent decisions have made it clear that the Court still recognizes the validity of state trade secret protection. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974); Goldstein v. California, 412 U.S. 546 (1973).

There is no federal trade secret legislation, although the need for such legislation has been recognized.[42] Nor does every state have trade secret legislation. Even in those states which do have such laws, misappropriation of a trade secret may not rise to the level of a crime. When a trade secret is taken, the form of the taking is often critical in determining whether prosecution is possible. This point will be dealt with in the sections below.

1. State Larceny Statutes.—In some instances, theft of computer programs is punishable as larceny. Common law larceny is the "felonious taking and carrying away of the personal property of another with intent to deprive the owner of his property permanently."[43] Special problems arise in applying this definition to misappropriation of computer programs with respect to the nature of the property taken, whether the property is carried away, and whether the owner is "permanently" deprived of something he retains possession of after his program is illicitly copied. Although many states by statute have altered the common law notion of larceny, one or more of these problems may still remain because statutory interpretation often involves application of common law principles.

Ms. Nycum believes that there are but two instances in which theft of a program may not be prosecutable as larceny.[44] The first occurs when the actor copies the program onto his own materials, for example, film, paper, or cards, but does not carry off the original.[45] In this instance, the original program is never brought under the direct or indirect control of the actor, and may not even be touched.[46] An indictment for larceny may also fail if the only thing taken is something as intangible as electronic impulses.[47] As Mr. Bender observed: "The nature of the entity which must be taken in order to constitute the crime is critical, and the precise wording and interpretation of the statute in question will determine whether the taking of a trade secret may constitute larceny."[48]

---

[42]*See, e.g.*, Keefe & Mahn, *Protecting Software: Is It Worth All the Trouble?*, 62 A.B.A.J. 906, 906-07 (1976).

[43]Fletcher v. State, 231 Md. 190, 192, 189 A.2d 641, 643 (1963), *quoted in* Bender, *supra* note 29, at 942.

[44]Nycum, *supra* note 27, at 275.

[45]Even though the act may not be prosecutable in some jurisdictions, it may be in others, particularly those in which the subject matter of larceny is anything of value. *See, e.g.*, IND. CODE § 35-43-4-2 (Supp. 1979).

[46]*See* note 37 *supra* and accompanying text.

[47]*See* Ward v. Superior Court, 3 COMPUTER L. SERV. REP. 206 (1972), *discussed at* text accompanying notes 67-72 *infra*.

[48]Bender, *supra* note 29, at 942.

Mr. Bender divides the fifty states and the District of Columbia into four groups according to the kind of property which can be the res of larceny or theft of a trade secret. The first group consists of those states which "follow the common law definition in defining the res as property, or by using some like phrase."[49] Mr. Bender offers little guidance as to what would happen concerning any purported theft of a trade secret in those states.[50]

Other states, those making up the second group, modify or extend the notion of property by providing lists which indicate what is to be considered "property."[51] Because laws dealing with criminal acts are to be interpreted strictly, the usual reading of these statutes would indicate that if a certain object could not be placed among the listed items, that object could not be the subject matter of theft.

The third group of jurisdictions is composed of those which hold the res of larceny to a "thing of value."[52] Computer programs ob-

---

[49]*Id.* Because Bender cites no authority for his conclusion, it is difficult to know how he arrived at it. A check of current state statutes dealing with theft and the definition of property relative thereto seems to reduce the list to two jurisdictions, Alaska and Idaho. ALASKA STAT. § 01.10.060(8) (1972); IDAHO CODE § 18-4601 (1972). *But see* IDAHO CODE § 55-102 (1972).

[50]There is so little case law in this area that speculation on the outcome of future cases is futile.

[51]Bender lists the following states: Alabama, Alaska, Arizona, Connecticut, Delaware, Iowa, Mississippi, Nevada, North Dakota, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Washington, West Virginia, and Wyoming. Bender, *supra* note 30, at 15 n.53. According to a more recent search of the statutes, "list" state statutes include MASS. GEN. LAWS ANN. ch. 266, § 30 (West Supp. 1979); MICH. GEN. LAWS ANN. § 750.10, .356 (1968); MISS. CODE ANN. § 1-3-41 (1972); NEV. REV. STAT. § 193.010 (1973); N.C. GEN. § 12-3 (1969); OKLA. STAT. ANN. tit. 21, § 103 (1958); R.I. GEN. LAWS § 11-41-1 (1970); S.C. CODE § 16-13-30 (1977); VT. STAT. ANN. tit. 13, § 2501 (1974); W. VA. CODE § 2-2-10 (1979); WIS. STAT. ANN. § 943.20 (West 1958 & Supp. 1979-80). In addition, a number of states use both a list and a definition of property as a "thing of value," or the like. Relevant statutes include: ARK. STAT. ANN. § 41-2201 (1976); GA. CODE ANN. § 26-401 (1978); HAWAII REV. STAT. § 708-800 (1976 & Supp. 1978); ME. REV. STAT. ANN. tit. 17A, § 352 (1979); MINN. STAT. ANN. § 609.52 (Supp. 1979); MONT. REV. CODES ANN. § 94-2-101 (1974 & Supp. 1977); N.H. REV. STAT. ANN. § 637:2 (1964 & Supp. 1973); N.Y. PENAL LAW § 155.00 (McKinney Supp. 1979-80); N.D. CENT. CODE § 12.1-23-10 (1960 & Supp. 1979); S.D. COMP. LAWS ANN. § 22-1-2 (1979); TEX. PENAL CODE ANN. tit. 7, § 31.01 (1974 Vernon); WYO. STAT. § 6-1-101 (1977).

Arizona has recently passed special legislation specifically addressed to computer crime. ARIZ. REV. STAT. ANN. § 13-2310(E) (1978). *See* text accompanying notes 157-61 *infra*. Prosecution for the same criminal act can, of course, often be pressed under more than one statute.

[52]The jurisdictions listed by Bender include the District of Columbia, Florida, Hawaii, Kansas, Louisiana, Maryland, Missouri, Montana, and Virginia. The exact phrase "thing of value" is not necessarily used in all of these jurisdictions, but Bender believes the respective phrases used are similar enough to mean the same things. Once again, Bender gives no authority. A search of statutes seems to indicate that "thing of

viously fit rather well under this rubric. Mr. Bender notes two problems which must be addressed not only in "thing of value" jurisdictions, but in those in the first two groups as well. The first problem arises when something is taken without an intent of permanently depriving its owner of possession, for example, when it is taken with the intent of replacing it after a copy has been produced. The intent to return, or the actual return of the object taken, may, in some jurisdictions preclude a charge of larceny, or might require that a lesser charge be filed. A second problem is establishing the value of the item taken. In *Hancock v. Texas*,[53] the value assigned to a set of misappropriated copies of programs was their commercial value as evidenced by expert testimony, but the defendant was prosecuted under a trade secret statute and not under the Texas larceny statute. If the value of the thing stolen is taken to be the value of the underlying material object, for example, the computer paper on which the program is printed, then someone stealing a program having a commercial value in the millions of dollars might be chargeable with only a trivial offense.

In addition to the two problems cited above, there is also the problem of the manner of theft. If the actor fails to make off with the program, or even move it, he has not deprived the owner of its possession, even for a brief moment. If the actor relies only on electronic signals, he may not have even made a tangible copy of the program. Of course, someone who misappropriates a copy of a program has by his action deprived the owner of something, specifically, the secrecy attached to the program as well as the potential commercial gain that might have been realized through the sale or licensing of the program. But not all courts would be willing to recognize secrecy or potential gain as property capable of being

---

value" is actually used in the following: ALA. CODE § 13A-8-1(10) (Supp. 1979); ARIZ. REV. STAT. ANN. § 13-105(27) (1956 & Supp. 1978); COLO. REV. STAT. § 18-4-401 (1973 & 1978 Repl.); CONN. GEN. STAT. ANN. § 53a-118(1) (West 1972); DEL. CODE ANN. tit. 11, § 877(4) (1974); D.C. CODE ENCYCL. § 22-2201 (West 1967); FLA. STAT. § 812.012(3) (1976 & Supp. 1979); ILL. REV. STAT. ch. 38, § 15-1 (1973); IND. CODE § 35-41-1-2 (1979); IOWA CODE § 702.14 (1976 & Supp. 1978); KAN. STAT. ANN. § 21-3110 (Supp. 1979); KY. REV. STAT. § 514.010(5) (1975); LA. REV. STAT. ANN. § 14:67 (West 1974); MD. ANN. CODE art. 27 § 340(h) (Supp. 1979); MO. ANN. STAT. § 570.010 (Vernon 1979); NEB. REV. STAT. § 28-509 (1943 & Supp. 1978); N.J. STAT. ANN. § 2c:20-2(g) (West Supp. 1979); N.M. STAT. ANN. § 30-16-1 (1978); OHIO REV. CODE ANN. § 2901.01 (Page 1975); OR. REV. STAT. § 164.005(5) (1979); 18 PA. CONS. STAT. ANN. § 3901 (Purdon 1972); TENN. CODE ANN. § 39-4201 (1975); TEX. PENAL CODE ANN. tit. 7, § 31.01 (Vernon 1974); UTAH CODE ANN. § 76-6-401(1) (1978); VA. CODE § 18.2-95 (1975); WASH. REV. CODE ANN. § 9A. 04.110(21) (1974). In addition, a number of statutes used both a list and "thing of value" to characterize property subject to theft. *See* note 49 *supra*.

[53]402 S.W.2d 906 (Tex. Crim. App. 1966), *aff'd sub nom.* Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967).

stolen, though interference with these rights may well form the basis for an action in tort.

The case of *Lund v. Commonwealth*[54] is instructive. Charles Lund, a doctoral student at Virginia Polytechnic Institute and State University (VPI), was convicted of grand larceny for use of VPI's computer without proper authorization. Lund's thesis research required the use of the computer, but, through an oversight, his advisor failed to provide an account for him. Lund began using accounts assigned to other persons and departments without their permission. The director of VPI's computer center estimated that by the time Lund was caught, he may have used as much as $26,384.16 in unauthorized computer time. The director also admitted that the value of the cards and paper obtained from Lund was "whatever scrap paper is worth."[55]

Lund admitted that he used the computer without specific authority, but he and four faculty members, including his department chairman and advisor, testified that the work was for his thesis and he would have been given authorization had he requested it. Lund appealed his conviction on the grounds that there was no evidence that the articles in question were stolen, or that they had a value of $100 or more, and, in any case, computer time and services were not the subject of larceny.

One of the Virginia statutes in question provided:

> Any person who: (1) Commits larceny from the person of another of money or other thing of value of five dollars or more, or
>
> (2) Commits simple larceny not from the person of another of goods and chattels of the value of one hundred dollars or more, shall be deemed guilty of grand larceny . . . .[56]

Another statute stipulated: "If any person obtain, by any false pretense or token, from any person, with intent to defraud, money or other property which may be the subject of larceny, he shall be deemed guilty of larceny thereof . . . ."[57]

The court found that "[a]t common law, labor or services could not be the subject of the crime of false pretense because neither time nor services may be taken and carried away."[58] Even though some states had amended their criminal codes to make obtaining

---

[54]217 Va. 688, 232 S.E.2d 745 (1977).

[55]*Id.* at 690, 232 S.E.2d at 747.

[56]*Id.* at 690, 232 S.E.2d at 747 (quoting VA. CODE § 18.100 (1950) (currently codified at VA. CODE § 18.2-95 (1975))).

[57]*Id.* at 690, 232 S.E.2d at 747 (quoting VA. CODE § 18.1-118 (1950) (currently codified at VA. CODE § 18.2-178 (1975))).

[58]217 Va. at 692, 232 S.E.2d at 748.

services by false pretenses a crime,[59] Virginia had not done so. Also, the unauthorized use of a computer was found not to be the subject of larceny because it did not involve the "taking and carrying away of a certain concrete article of personal property."[60] The court also would not accept the Commonwealth's argument that the value of the print-outs should be measured by the cost of production. The court concluded that where there is no market value for an article that has been stolen, the prosecution must prove its value.[61] The print-outs had no ascertainable value to VPI or the computer center. Lund's conviction was reversed and the indictment quashed.[62]

2. State Trade Secret Legislation.—A group of states have passed legislation which deals specifically with trade secrets. At the time of Mr. Bender's first survey,[63] eighteen states had passed such legislation; six years earlier none had.[64] By the time of his updated article in 1977,[65] twenty-one states had such legislation.[66] The fact

---

[59]See, e.g., N.Y. PENAL CODE § 165.15 (McKinney, Supp. 1979-80); N.J. REV. STAT. § 2A:111 (1969) (currently codified at N.J. REV. STAT. § 2C:208 (Supp. 1979)); CAL. PENAL CODE § 487 (West 1970).

[60]217 Va. at 692, 232 S.E.2d at 748.

[61]*Id.*

[62]*Id.* at 693, 232 S.E.2d at 749. The result in this case seems entirely just and reasonable, but suppose Lund had been playing "Startrek" instead of working on his thesis, or using the VPI computer for private gain, perhaps doing other students' programming assignments for pay?

[63]Bender, *supra* note 29.

[64]*Id.* at 947 n.200.

[65]Bender, *supra* note 30.

[66]Bender lists Arkansas, California, Colorado, Georgia, Illinois, Indiana, Maine, Massachusetts, Michigan, Minnesota, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Tennessee and Wisconsin, finally citing some authority for his statements. Specific statutes are listed in Bender, *supra* note 30, at 17 nn.64-67. The state law is often difficult to classify. The situation in Indiana illustrates this point. In 1969 the Indiana General Assembly added §§ 35-17-3-1 to -5 to the Indiana Code. These statutes described theft or embezzlement of an article representing a trade secret as well as copying an article representing a trade secret. They required an intent to deprive the owner of the secret of its control, or an intent to appropriate the secret to the actor's use or to the use of a third party. Return or intent to return was no defense. Nevertheless, in these statutes, the definitions of "article" and "copy" both implied some tangible object. In the 1976 revision of the criminal code, this separate chapter dealing with trade secrets was repealed, and trade secrets were incorporated into the definition of "property" listed in IND. CODE § 35-41-1-2 (Supp. 1979). Although § 35-41-1-2 describes property as "anything of value," it also names various types of property with some specificity. Thus, there is an ambiguity as to whether the specific is intended to prevail over the general inasmuch as there are articles which have value which do not seem to fit under any of the headings. In accordance with the usual strict interpretation of criminal statutes, it would seem that the more restrictive meaning of property should govern. But, by the

that a state has a statute which makes criminal a misappropriation of a trade secret does not preclude prosecution under other laws, such as the larceny statute, for the same offense.

As one might expect, California and New York, because of their size and the complexity of their technology and industry, have trade secret statutes. California, in fact, has one of the most detailed such statutes in the nation.[67] This statute provides in part:

> (b) Every person is guilty of theft who, with intent to deprive or withhold from the owner thereof the control of a trade secret, or with an intent to appropriate a trade secret to his own use or to the use of another, does any of the following:
>
> (1) Steals, takes, or carries away any article representing a trade secret.
>
> (2) Fraudulently appropriates any article representing a trade secret entrusted to him.
>
> (3) Having unlawfully obtained access to the article, without authority makes or causes to be made a copy of any article representing a trade secret.
>
> (4) Having obtained access to the article through a relationship of trust and confidence, without authority and in breach of the obligations created by such relationship makes or causes to be made, directly from and in the presence of the article, a copy of any article representing a trade secret.[68]

The statute further proscribes conspiracy to obtain a trade secret,[69]

---

doctrine of plain meaning, it could also be argued that the list of objects is merely illustrative and not exhaustive. Which Bender category fits Indiana? Is Indiana a "thing of value" state, one which has a list, or one which has specific legislation addressed to trade secrets by virtue of its listing trade secrets explicitly in its criminal code? There is now some guidance in this area because of the *Thommen* case which is discussed later.

The law in Indiana concerning valuation of property and the sort of asportation required to sustain a conviction for theft is also unclear. In Warnke v. State, 89 Ind. App. 683, 167 N.E. 138 (1929), the conviction of an inept chicken thief who fled the coop leaving his bag of chickens behind was upheld. *Id.* at 686, 167 N.E. at 139. Early Indiana cases indicate that the collective value of all items stolen may be totaled to make the actor liable for larceny of a higher degree than he would have been for the theft of any individual item. *E.g.*, Edson v. State, 148 Ind. 285, 47 N.E. 625 (1897). Concerning value, the new Indiana Criminal Code requires only that whatever is taken have some value. IND. CODE § 35-41-1-2 (Supp. 1979). The extent of the value may not have to be proved. *See* text accompanying note 178 *infra*.

[67]CAL. PENAL CODE § 499c (West 1970 & Supp. 1979).

[68]*Id.* § 499c(b).

[69]*Id.* § 499c(c).

and explicitly declares that the return or intent to return the article representing the trade secret is not a defense.[70]

Despite its precision and comprehensiveness, the California statute leaves possible loopholes for the computer thief because both "article" and "copy" as defined elsewhere in the statute seem to refer only to tangible objects.[71] Furthermore, even though the conspiracy portion of the statute may cover a situation where an employee memorizes a program, copies outside his place of employment what he has memorized, and then delivers it for consideration to a third party, the law does not seem to forbid the employee from using the memorized program for his own personal benefit.[72]

Theft of a trade secret may also be prosecuted under the California larceny statute.[73] Even though the larceny statute does not explicitly state that trade secrets may be the object of larceny, California case law indicates that prosecution for theft of a trade secret may be maintained under the larceny statute provided that the secret is represented by some tangible object which has been carried away.[74] The valuation used is the commercial value and not the intrinsic value of the underlying object.[75]

In *Ward v. Superior Court*,[76] Ward, an employee of a computer service bureau,[77] used a telephone to transfer a secret program from a competitor's computer to that of his employer. He then caused his employer's computer to print a copy of the stolen program, which he carried to his office.[78] He was charged under both the trade secret[79] and grand theft statutes[80] of California. The court found that the

---

[70]*Id.* § 499c(d).

[71]For example, "article" is defined as "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." *Id.* § 499c(a).

[72]*See* Bender, *supra* note 29, at 947-50.

[73]CAL. PENAL CODE § 484a (West 1970).

[74]People v. Dolbeer, 214 Cal. App. 2d 619, 29 Cal. Rptr. 573 (1963). *Dolbeer* involved a prosecution under the larceny statute for theft of lists of telephone subscribers. It was important to the court that some tangible object was taken. Indeed, the court stated that had the lists been merely copied in some manner, but not carried off, the prosecution could probably not have been upheld. *Id.* at 623, 29 Cal. Rptr. at 575.

[75]*Id.* at 622-24, 29 Cal. Rptr. at 574-75.

[76]3 COMPUTER L. SERV. REP. 206 (1972).

[77]A computer service bureau is a firm which supplies computer services, including actual machine use, to its clients.

[78]In doing so, Ward fraudulently used another client's account number. It appears that charges were not pressed on these grounds. If the client whose number was used actually incurred charges due to the fraudulent use, Ward might have been prosecuted for theft from, or fraud upon, that party as well. 3 COMPUTER L. SERV. REP. at 210.

[79]CAL. PENAL CODE § 499c(b) (West 1970 & Supp. 1979). *See* text accompanying note 68 *supra*.

[80]*Id.* § 487.

"article" taken must be tangible, "even though the trade secret which the article represents may itself be *intangible*."[81] Although the electronic impulses representing the stolen program were not sufficiently tangible to constitute an article of theft,[82] Ward had gone beyond merely transferring electronic impulses from one computer to another. His act of making a tangible copy of the program and then carrying the copy even the short distance to his office sufficed to establish the elements necessary for prosecution. Furthermore, merely making the copy in itself was a violation of the trade secret statute.[83] The court also concluded that the enactment of the trade secret statue made a trade secret property which is subject to theft. Therefore, a misappropriation of any trade secret, or article representing a trade secret, can also be charged as a theft of property under the larceny statute.[84] The lesson for potential computer thieves, at least in California, is that they should not make tangible copies of the programs they steal. If Ward had merely transferred the competitor's program to his computer and used it, possibly to his great profit, without bothering to print it, he might not have been subject to prosecution.

The New York larceny statute includes both trade secrets and "secret scientific materials."[85] Copying is itself an offense prosecutable apart from, or in addition to, stealing.[86] New York also appears to have a very broad notion of property which may be subject to theft.[87] A New York court described a prior, similar statute as follows: "It is difficult to conceive a definition more comprehensive than this, for it includes intangible property, as well as tangible, written instruments, as such, and everything, except real property, that is capable of being owned or transferred."[88] New York seems to follow the same valuation rule as California and Texas, that is, the commercial value of the object taken governs.[89]

3. Model Penal Code.—The Model Penal Code has virtually as broad a definition of property as does New York,[90] but the notion of

---

[81]3 COMPUTER L. SERV. REP. at 208.

[82]*Id.*

[83]CAL. PENAL CODE § 499c(b)(3) (West 1970 & Supp. 1979). *See* note 68 *supra* and accompanying text.

[84]3 COMPUTER L. SERV. REP. at 210-11.

[85]N.Y. PENAL LAW § 155.30(3) (McKinney 1975).

[86]Nycum, *supra* note 27, at 279.

[87]N.Y. PENAL LAW § 155.00(1) (McKinney 1975).

[88]*In re* Bronson, 150 N.Y. 1, 5, 44 N.E. 707, 711, 110 N.Y.S. 949, 954 (1896) (Vann, J., dissenting).

[89]*See, e.g.*, People v. Irrizari, 5 N.Y.2d 142, 156 N.E.2d 69, 182 N.Y.S.2d 361 (1959).

[90]MODEL PENAL CODE § 223.0(6) (Proposed Official Draft, 1962).

theft includes depriving the owner of either the property or some legal interest therein, either permanently or for some extended period of time.[91] If the right to secrecy or the right to payment for use of a program is "property" in the sense the Code intends (and it quite reasonably could be so interpreted), misappropriation of a program could be prosecuted as theft under the Code. The Code also has a section which defines the offense of theft of services which might be stretched to prosecute someone who knowingly or fraudulently obtains computer services of any sort without any intent of paying for them.[92] The value of property stolen is taken to be the "highest value, by any reasonable standard" of that property;[93] thus, the commercial value of a purloined program would certainly be admissible.

4. Federal Law.—The principal federal statute related to theft, section 641 of title 18 of the United States Code, is quite comprehensive concerning the acts covered and the res required.[94] Forbidden activity includes embezzling,[95] stealing, knowingly converting to the use of the actor or a third party, as well as selling, disposing of, or conveying without authority "anything of value" which belongs to the United States or any department or agency thereof, or even any property which has been made or is being made under contract for the United States or any of its departments. The statute also proscribes receiving and hiding stolen property if it is known to have been stolen.

Stealing is a narrower notion than conversion. The Supreme Court has drawn the following distinction:

> To steal means to *take away from one* in lawful possession without right with the *intention to keep* wrongfully . . . .

---

[91] *Id.* §§ 223.0(1), (5), .2(1).

[92] *Id.* § 223.7.

[93] *Id.* § 223.1(2)(c).

[94] The statute provides for a fine and imprisonment for:

> [Whomever] embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of . . . anything of value of the United States or any department or agency thereof, or any property made or being made under contract for the United States or any department thereof, or whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted . . . .

18 U.S.C. § 641 (1976).

[95] Embezzlement is fraudulent or felonious conversion or appropriation of property which has *rightfully or lawfully* come into the converter's possession. For a fairly comprehensive discussion of embezzlement and § 641, see United States v. Powell, 294 F. Supp. 1353 (E.D. Va. 1968), *aff'd per curiam*, 413 F.2d 1037 (4th Cir. 1969).

> Conversion, however, may be consummated without any intent to keep and without any wrongful taking, where the initial possession by the converter was entirely lawful. Conversion may include misuse or abuse of property.[96]

The Court of Appeals for the Third Circuit interprets the Supreme Court as saying that section 641 applies when anyone obtains a wrongful advantage from the property of another.[97] Section 641 has also been used to successfully prosecute an army officer who used the services of government employees for his own personal gain.[98]

The phrase "of the United States or of any department thereof" is to be interpreted with great latitude as well. For example, if the government has a license for the use of certain programs, theft of the programs would suffice to invoke federal jurisdiction. "In its broadest interpretation, any misappropriation of software which is subject to some measure of government control, custody, or ownership is a violation of section 641."[99] The measure of value of any item misappropriated is the "face, par, or market value, or cost price, either wholesale or retail, whichever is greater."[100] This implies that the commercial value of a stolen program would be accepted by a court as a measure of its worth. If the program were completely lost to its owner, the cost of rewriting it might be acceptable.

Other federal statutes also apply to theft-related offenses. Section 659 of title 18, for example, deals with theft from an interstate common carrier, and applies regardless of who owns the goods stolen: "The interstate character of a shipment commences at the time that the property is segregated for interstate commerce [such character continuing] until the property arrives at its destination and is there delivered either by actual unloading or by being placed to be unloaded."[101] The particular act proscribed by this statute is more limited than that covered by section 641. Although the required intent is the same as that for conversion, the act in question must be theft or embezzlement.[102] The act does not seem to cover unauthorized copying. Section 2314 of title 18 also forbids interstate transportation of stolen property. The stolen article must actually cross state lines to trigger this statute. In *United States v. Lester*,[103]

---

[96]Morissette v. United States, 342 U.S. 246, 271-72 (1952) (citing Irving Trust Co. v. Leff, 253 N.Y. 359, 364, 171 N.E. 569, 571 (1930)).

[97]United States v. Crutchley, 502 F.2d 1195, 1201 (3d Cir. 1974).

[98]Burnett v. United States, 222 F.2d 426, 427 (6th Cir. 1955).

[99]Nycum, *supra* note 33, at 306.

[100]18 U.S.C. § 641 (1976).

[101]United States v. Astolas, 487 F.2d 275, 278 (2d Cir. 1973).

[102]This interpretation is strongly implied by the language in United States v. Astolas, *id.* at 279. *See also* Nycum, *supra* note 33, at 307.

[103]282 F.2d 750 (3d Cir. 1960).

a conviction was upheld even though the defendant had merely transported misappropriated copies of commercially valuable geological survey maps across state lines.[104] This decision implies that section 2314 could perhaps be invoked if someone carried an unauthorized copy of a computer program across state lines. Other federal laws, such as that which covers conversion by a government employee of property entrusted to his care,[105] may also be helpful in curbing computer crime in certain carefully defined situations.[106]

C. Other Federal and State Statutes

Although theft of software constitutes one of the largest potential sources of loss due to computer crime, there are other ways to lose than by theft and other ways to misappropriate things than by simply carting them off. A common problem at university computing facilities, for example, is unauthorized use of the machine, that is, misappropriation of computer time and resources. Because these are "things of value," it is likely that, even in this case, many state larceny statutes might be applicable. There are usually other state statutes which could be used to handle this situtation, at least if a court can be convinced to interpret such statutes in a reasonable, though possibly broad, manner. For example, even an unauthorized user must usually provide an account number to which his use of computer resources will be charged. Furnishing this information is, in effect, fraudulently tendering a credit card because the account the user is tendering is not his own.[107] This practice can lead to prosecution under a credit card fraud statute.[108]

Damaging information that is stored on magnetic tape, for example, garbling the information by passing it through a strong magnetic field, is almost certainly prosecutable under a malicious mischief statute, provided that the court can be apprised of the precise nature of the damage done.[109] If anyone breaks and enters a computer facility with the express purpose of doing substantial damage or committing some other felony, he is, of course, subject to prosecution for burglary as well.[110]

Some states have "telephone abuse" statutes which might be used to prosecute someone who attacks a computer or its contents from a

---

[104]*Id.* at 754-55.

[105]18 U.S.C. § 654 (1976).

[106]*See* 18 U.S.C. §§ 285, 655-57, 1707, 2113 (1976).

[107]If a false name or identification is used, forgery might also be involved. This raises the question of what constitutes a "signature" in dealing with a computer. The question is not without importance in view of the arrival of electronic funds transfer.

[108]*See, e.g.*, IND. CODE § 35-43-5-4 (Supp. 1979).

[109]*See, e.g., id.* § 35-43-1-2.

[110]Criminal trespass might also apply. *See, e.g., id.* § 35-43-2-2.

remote site via a telephone line. Although the laws of each state are different, there is no state which does not already have a substantial arsenal of statutes dealing with larceny, fraud, and invasion of privacy which can be used against the computer criminal. Other statutes dealing with credit card fraud, fraudulent destruction of recordable instruments,[111] or tampering with records[112] might also prove to be valuable weapons.

Other federal laws besides those related directly to larceny can also be employed against computer crime.[113] The two principal statutes which deal with abuse of federal channels of communication are sections 1341 (mail fraud) and 1343 (wire fraud) of title 18. Both statutes have two essential elements: 1) the actor must use the mail (wire) for the purpose of executing, or attempting to execute, 2) a fraud or scheme to obtain money or property under false pretenses. Fraud has been liberally interpreted by the federal courts, and it is likely that they would find fraud in a scheme to obtain an unauthorized copy of a program. All cases tried to date under the wire fraud statute have involved calls which have crossed state lines.[114]

One such wire fraud case was *United States v. Seidlitz*.[115] Seidlitz, who operated his own computer business in Virginia, had obtained access codes to the computer of a former employer, Optimum Services, Inc. (OSI), located in Rockville, Maryland. OSI had developed a sophisticated program that Seidlitz misappropriated for his own personal gain. He obtained the electronic signals which represented the program through interstate telephone lines. Once the transmission had been made, he could, of course, print copies of the program from the stored information. Seidlitz also had a computer terminal in his home in Maryland. As events turned out, he would have been better off had he stolen the programs using that terminal. Seidlitz's thievery was discovered, as are most such computer crimes, purely by accident.

---

[111]MODEL PENAL CODE § 224.3 (1962).

[112]*Id.* § 224.4.

[113]Nycum classifies the federal statutes under seven broad headings: 1) theft and related crimes, 2) abuse of federal channels of communication, 3) national security offenses, 4) trespass and burglary, 5) deceptive practices, 6) malicious mischief and related offenses, and 7) miscellaneous other statutes. Nycum, *supra* note 33, at 305. This general order will be followed here.

[114]Nycum, *supra* note 33, at 311-12.

[115]This is an unreported case discussed in SECURITY, *supra* note 20, at 234. The report and analysis of this case were submitted to the Committee on Governmental Operations by Mr. Jervis Finney, U.S. Attorney for the District of Maryland, the jurisdiction within which the crime occurred.

Mr. Jarvis Finney, in a report to the Senate Committee on Governmental Affairs, pointed out some of the serious problems associated with trying to win a conviction in this kind of case under existing state and federal law.[116] First, there is the problem of proving that Seidlitz actually called the computer from which he was stealing programs. Having established this, "it is also incumbent to establish, with precision, what material is being retrieved from the computer. Unless the victim company has certain specialized equipment available, this may pose an extreme burden which can seriously hamper any attempt to obtain a search warrant."[117]

If it had been determined that Seidlitz had indeed phoned OSI's computer and that OSI knew precisely what information had been transmitted to Seidlitz's phone, a search of his premises may have revealed no identifiable copies. The evidence could have been entirely concealed on magnetic tapes or in invisible electronic switches at the heart of his computer. The program could have been scrambled in such a way that only Seidlitz could decode it by means of another secret program; hence, an exhaustive search of his home and business might have revealed no clear evidence of any crime, even if the entire contents of his computer's memory had been "dumped" and given to a computer specialist to read.[118] Such a blanket seizure and examination of all of Seidlitz's records and all of the information stored in his computer, however, might have run afoul of the fourth amendment.

If Seidlitz had not transmitted the programs to Virginia, the wire fraud statute would have been useless. Moreover, a charge of interstate transportation of stolen property was dismissed due to a lack of asportation. The programs that Seidlitz misappropriated were not really carried off; they still resided inside OSI's computer. Seidlitz had merely reproduced them by means of an electronic signal over the phone. The case was thus distinguishable from those in which a copy had first been made and then transported interstate.

A conviction for what must appear to most sensible people to be a crime was nearly avoided because what was stolen was not carried off. Whether the court would have found asportation if he had erased the program in OSI's computer at the same time he copied it into

---

[116]Unfortunately, many prosecutors faced with similar difficulties would not have attempted any prosecution, perhaps suggesting a suit in tort as a remedy for the injured party.

[117]SECURITY, *supra* note 20, at 235.

[118]Inasmuch as computer systems can hold information equivalent to miles of printed copy, the sheer task of searching for the evidence is like looking for the proverbial needle in the haystack.

his own is a matter of conjecture. It would certainly seem that the gratuitous destruction of OSI's program should not be required to classify Seidlitz's act as a theft. The courts would do well to reexamine the concept of asportation in situations such as this.

There are rather specialized statutes which relate to national security.[119] The broadest of these, section 793(f) of title 18, seems to proscribe virtually any malfeasance having to do with information or documents related to national security, including the knowing failure to report the loss of such a document.[120]

Federal statutes concerning trespass and burglary refer to specialized areas, such as banks and post offices, and not to the more general notion of "federal enclave."[121] It appears that section 2113(a) of title 18, which deals with robbery of a bank, refers only to common law larceny[122] and not to a more extensive notion that might enable a court to find larceny in misappropriation of a trade secret. The Supreme Court, moreover, has held that federal criminal law in this respect is not to be interpreted in the light of state law.[123] Thus, these statutes are not as helpful in prosecuting computer crime as they may first appear. The Assimilative Crimes Act, however, adopts state penal law to fill in the gaps in federal law for each federal enclave in the state.[124] Thus, even though federal law may be deficient when considered in isolation, state law may remedy that deficiency.

Several federal statutes relate to deceptive practices,[125] but by far the most comprehensive of these is section 1001 of title 18.[126] All that section 1001 requires is some "false, fictitious or fraudulent statement, knowingly and willfully made." The statute applies to both oral and written representations.[127] Because an entry of a

---

[119]18 U.S.C. §§ 793-95, 797-99, 952 (1976).

[120]*Id.* § 793(f).

[121]*See Id.* § 7 for the definition of federal property for purposes of the criminal code.

[122]The statute was so construed in United States v. Rogers, 289 F.2d 433, 437 (4th Cir. 1961).

[123]Jerome v. United States, 318 U.S. 101, 106 (1943).

[124]*See* note 36 *supra* and accompanying text.

[125]18 U.S.C. §§ 912, 1001, 1005, 1006 (1976).

[126]Section 1001 provides in part:

> Whoever, in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme or device a material fact, or makes any false, fictitious, or fraudulent statements or representations or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be fined . . . .

18 U.S.C. § 1001 (1976).

[127]United States v. Zavala, 139 F.2d 830, 831 (2d Cir. 1944).

password or authorization code into a computer is a statement that the one who enters it is entitled to what he orders the computer to give him, this statute would seem to be a likely weapon with regard to misappropriation of computer services or information stored in a computer in any case in which the actor misrepresents his identity or his status.

An instructive case relating to computer abuse by fraud is *United States v. Jones.*[128] Through a sophisticated scheme, again discovered solely by chance, the defendant's brother had a computer generate checks payable to the defendant which should have been payable to the defendant's employer. Because the payor on these checks was Canadian, the defendant was charged with transporting foreign commerce checks valued at more than $5,000, knowing the checks had been taken by fraud,[129] and of unlawfully converting these checks knowing them to be fraudulent.[130] The defendant moved that the indictments be dismissed on the grounds that the checks in question were actually forgeries and, therefore, did not fall under the provisions of the statutes under which she was charged.[131] The district court held that the checks were indeed forgeries and dismissed the indictments;[132] the government appealed.

The legal issue on appeal was whether "the alteration of accounts payable documents fed into a computer which resulted in the issuance of checks payable to an improper payee constituted a 'falsely made, forged, altered, counterfeited or spurious' security."[133] The Court of Appeals for the Fourth Circuit reversed the district court, holding that the acts which caused the computer to print the fraudulent "checks did not constitute the making of a false writing, but rather amounted to the creation of a writing which was genuine in execution but false as to the statements of fact contained in such writing."[134]

The prosecuting attorney pointed out that if the checks had been found to be forgeries, and the indictments had been dismissed, then there would probably have been no federal statutes under which the defendant could have been charged.[135] The mail fraud

---

[128]553 F.2d 351 (4th Cir. 1977), *cert. denied*, 431 U.S. 968 (1977). This case is discussed in SECURITY, *supra* note 20, at 236-37.

[129]18 U.S.C. § 2314 (1976).

[130]*Id.* § 2315.

[131]The statutes did "not apply to any falsely made, forged, altered, counterfeited or spurious representation of an obligation or . . . promise to pay . . . by a bank or corporation of any foreign country." 553 F.2d at 352 n.2.

[132]United States v. Jones, 414 F. Supp. 964, 971 (D. Md. 1976).

[133]553 F.2d at 354.

[134]*Id.* at 355.

[135]SECURITY, *supra* note 20, at 238. *See* note 103 *supra.*

statute might have been the only other possibility, but it would have required some proof that checks were placed in the mail in a scheme to defraud, whereas no checks might have been sent through the mail. "Thus, there may be instances where computer-related criminal activity has no criminal sanction."[136]

Federal statutes which deal with the destruction of property seem well-styled to handle a broad spectrum of possible offenses;[137] section 1361, which deals with the malicious destruction of government property, is the widest in its scope. It has been used in a case in which blood was poured on selective service records.[138] In that case, the value of the property injured was taken to be the cost of restoring the damaged records.[139]

Despite the seeming availability of statutory protection, prosecution of computer "criminals" is often difficult. This point is illustrated by testimony given by Ms. Susan Nycum before a Senate subcommittee in which she related a personal experience concerning computer abuse which might not have been prosecutable.[140] While Ms. Nycum was in charge of a computer center, one of her staff detected a user attempting to erase the volume table of contents for the system. The destruction of this master file would have created havoc in the computer operations. According to Ms. Nycum's estimate, it would have cost $50,000 to recreate the file. The attempt at destruction was made from a terminal outside the computer center itself using intrastate telephone lines and was frustrated only because of prompt action taken to disconnect the caller. Despite the large amount of damage and incovenience that would have resulted had the attempt succeeded, local law enforcement agencies were not sure that there was any law under which they could prosecute. The best they could do was suggest that the perpetrator be charged with making an obscene phone call. No charges were filed. Though state authorities were involved in the incident, it is not clear that under the circumstances federal authorities would have had an option of prosecuting even for an obscene phone call.

Some miscellaneous federal crimes with which a computer criminal could be charged include aiding and abetting a criminal,[141] assisting the actor after the commission of the crime as an accessory after the fact,[142] and conspiracy.[143] A government employee can be

---

[136]SECURITY, *supra* note 20, at 238.

[137]18 U.S.C. §§ 81, 1361, 1363, 2071, 2153, 2155 (1976).

[138]United States v. Eberhardt, 417 F.2d 1009 (4th Cir. 1969).

[139]*Id.* at 1013.

[140]*Hearings*, *supra* note 6, at 70.

[141]18 U.S.C. § 2 (1976).

[142]*Id.* § 3.

[143]*Id.* § 371.

charged with disclosure of confidential information if he discloses secret software in government custody, even if the software is owned by a private party and not the government.[144] In addition, the notion of fraud upon the government is very broad and does not imply pecuniary loss to the government.[145] It is somewhat odd that there is no general federal statute which states that it is a crime to defraud the government; thus, as Ms. Nycum points out, the conspiracy statute makes criminal an act of planning to do something which is itself not criminal.[146]

III. New Legislation

There are already a respectable number of state and federal laws which can be used to combat computer crime. The unique nature of computers, however, poses certain problems in the application of these laws in certain instances. At least two states have passed special legislation to deal with computer abuses, and Congress, along with several states, is considering such legislation. Consideration of this legislation forms the concluding part of this Article.

A. Federal Computer Systems Protection Act

Florida and Arizona have each passed laws specifically directed against computer crime; similar legislation is under consideration elsewhere,[147] and a "Federal Computer Systems Protection Act of 1979" is before the United States Senate.[148] The Senate bill describes the proscribed acts as follows:

> (a) Whoever knowingly and willfully, directly or indirectly accesses, causes to be accessed or attempts to access any computer, computer system, computer network, or any part thereof which, in whole or in part, operates in interstate

---

[144]Haas v. Henkel, 216 U.S. 462 (1910).

[145]Nycum, *supra* note 33, at 320.

[146]18 U.S.C. § 1905 (1976).

[147]*See, e.g., California DP Crime Bill Delayed for Redraft*, Computerworld, Mar. 12, 1979, at 14; Whitemarsh, *Colo. Crime Bill Expected to Pass*, and *DP Crime Legislation: A State-by-State Scorecard*, Computerworld, May 21, 1979, at 1. For examples of recent computer crime legislation, *see* Ala. Code § 13A-8-10(b) (1979); Cal. Penal Code § 502 (West 1979); 1979 Ill. Legis. Serv. P.A. 81-548 (West); 1979 N.C. Adv. Legis. Serv. No. 7, C. 831; Utah Code Ann. § 76-6-701 to -704 (Supp. 1979).

[148]S. 240, 96th Cong., 1st Sess., 125 Cong. Rec. S709 (daily ed. Jan. 25, 1979). This was originally Senate Bill S. 1766, the "Federal Computer Systems Protection Act of 1977." Although most witnesses at the hearings on this bill felt that new legislation was needed, almost no one was satisfied with the bill itself. Senator Ribicoff redrafted the bill, incorporating certain suggestions of then Assistant Attorney General Benjamin Civiletti. Cong. Rec. at S719-24. *See Hearings, supra* note 6.

> commerce or is owned by, under contract to, or in conjunction with, any financial institution, the United States Government or any branch, department or agency thereof, or any entity operating in or affecting interstate commerce, for the purpose of:
> (1) devising or executing any scheme or artifice to defraud, or
> (2) obtaining money, property, or services, for themselves or another, by means of false or fraudulent pretenses, representations or promises, shall be fined a sum not more than two and one-half times the amount of the fraud or theft or imprisoned not more than 15 years or both.
> (b) Whoever intentionally and without authorization, directly or indirectly accesses, alters, damages, destroys, or attempts to damage or destroy any computer, computer system, or computer network described in subsection (a), or any computer software, program or data contained in such computer, computer system or computer network, shall be fined not more than $50,000 or imprisoned not more than 15 years or both.[149]

The bill continues with an extensive and fairly complex list of definitions. "Access" is defined so broadly that it could include the use of almost anything having something to do with a computer.[150] On the other hand, the definition of "computer" is both too narrow and too broad. It is limited to electronic devices which manipulate data via electronic or magnetic impulses, thus excluding some of the major new forms of computers,[151] yet the definition is not restricted to general purpose machines, thus opening the way for rulings that electronic watches and automated traffic signals are covered by the bill.[152] Moreover, because the notion of computer is extended to "all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system

---

[149]125 CONG. REC. at S709.

[150]"'Access' means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network." *Id.* at S710.

[151]*Hearings*, *supra* note 6, at 67 (testimony of D. Parker).

[152]*See id.* Apparently the Senate Criminal Justice Subcommittee found the definition too broad as well. In the version voted out of that committee on November 6, 1979, automated typewriters, home computers and hand-held calculators were specifically exempted. In place of the many paragraphs of definitions dealing with computers, computer systems, computer networks, and so forth, the committee defined a computer as "a device that performs logical, arithmetic and storage functions by electronic manipulation and includes any property and communication facility directly related to or operating in conjunction with such a device." *DP Crime Bill Progresses in Senate*, COMPUTERWORLD, Nov. 19, 1979, at 2, col. 2 [hereinafter cited as *DP Crime Bill*].

or network,"[153] it appears that software and even telephones are to be treated as part of the computer itself. Yet, despite this seeming breadth, it appears that one of the most serious potential sources of loss, illicit photocopying of a printed program, is not covered at all.

The Senate bill is inadequate for two reasons. First, the proposed legislation duplicates much existing legislation. Second, and almost antithetical to the first conclusion, this bill ranges so broadly and is written so unclearly that it is hard to say with any degree of certainty exactly what the bill proscribes. Because its penalties are rather severe—up to fifteen years in prison for perhaps twenty-five cents worth of misappropriated computer time—the legislation should be more specific concerning what actions it covers.

The scope of federal jurisdiction is one of the most striking features of the bill. It seems even broader than section 641 of title 18, which is quite broad indeed.[154] For example, a state university computer which is used, even in small part, to process data in conjunction with some federally funded research project, would apparently be protected by the bill. Thus, a student having no connection with any federal program might be subject to federal prosecution and fifteen years in jail for causing such a computer to print out some obscene comment on a terminal. There is scarcely any computer operation of any size which is not likely to fall under the protection of the bill. Carried to its extreme, this bill will cover a theft of an electronic wristwatch in interstate commerce, and might even cover running a red traffic light.[155]

Another serious problem is the bill's ambiguity regarding what actions constitute a crime. It is common practice within computer operations to attempt to devise ways to beat the system, cause it to "crash," or obtain data to which they are not entitled. Some computer operations tolerate such antics, even though the consequences can be annoying, because it helps them locate and correct security flaws. It is virtually standard practice as well, particularly with university systems, for students to play unauthorized games such as

---

[153]125 CONG. REC. at S710.

[154]*See* notes 94-100 *supra* and accompanying text. The Senate Criminal Justice Subcommittee's version submitted to the full Senate Committee on the Judiciary now "covers all computers used by the federal government, by financial institutions or in interstate commerce." *DP Crime Bill*, *supra* note 134, at 2, col. 2. This version is still very broad.

[155]An automated traffic light, particularly one which is attached to a computer which counts cars and times the cycle of red and green, is part of a computer system as defined by this bill. If the traffic light controls traffic on a heavily traveled interstate route, it is arguably operating in interstate commerce. Absurd as it may seem, a driver who runs a red light could be charged with unauthorized access to, or alteration of, the system. The Senate Subcommittee which considered S.240 did try to make some changes that addressed some of these problems. *See* note 152 *supra*.

"Star Trek," print "Snoopy" calendars or pictures of the Mona Lisa, compile statistics for bowling leagues, or do other jobs that the rules of the system definitely forbid. These rules, however, are virtually unenforceable, and abuses are sometimes winked at to encourage students to gain greater experience in the use of the computer. Punishment of a $50,000 fine and fifteen years in jail for such pranks clearly seems excessive.[156] It is also doubtful that the bill could survive a constitutional challenge on the grounds of vagueness.

B. The Arizona Statute

The definition of the relevant computer-related terminology in the Arizona statute[157] is quite similar to that of Senate bill 240 and thus suffers from the same defects. The main body of the legislation creates a new crime, computer fraud:

> A. A person commits computer fraud . . . by accessing, altering, damaging or destroying without authorization any computer, computer system, computer network, . . . with the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses, representations or promises.
> B. A person commits computer fraud . . . by intentionally and without authorization accessing, altering, damaging or destroying any computer, computer system or computer network or any computer software, program or data contained in such computer, computer system or computer network.[158]

Although the scope of this statute is not quite as broad as the Senate bill, it suffers from many of the same ailments. It is not clear what acts are specifically forbidden, and the Arizona Attorney General has admitted that student use of computer time without authorization would be a violation. He would rely on prosecutorial discretion to avoid abuse of the law.[159] As was the case with Senate bill 240, the law does not seem to make unauthorized copying of a program a crime under many common circumstances.

The Arizona law suffers from yet another defect. Some of the terms in the new law are defined in pre-existing statutes. The com-

---

[156]The latest version of the bill (amended in subcommittee) reduced the penalties to a fine "of two times the amount lost or $50,000, whichever is higher and/or five years in jail," to bring them into line with the federal wire and mail fraud statutes. *DP Crime Bill*, *supra* note 152, at 2, col. 2.

[157]ARIZ. REV. STAT. ANN. § 13-2316 (1978).

[158]*Id.*

[159]*Hearings*, *supra* note 6, at 143.

puter fraud statute speaks of the "intent to . . . control property."[160] In section 13-1801, which deals with definitions related to theft, "control" is defined as an act by a defendant which excludes an owner from using his property except on the defendant's own terms.[161] In stealing a copy of a program for personal use, an actor would not control the program in this sense. Arizona courts will have to determine whether the new law has actually extended the notion of control.

C. The Florida Statute

Florida has chosen to use definitions similar to those proposed by the Association for Computing Machinery (ACM), the largest organization of computer professionals in the world.[162] "Computer" is defined in the Florida Crimes Act[163] as "an internally programmed, automatic device that performs data processing."[164] Similar to the ACM definition, the definition is, unfortunately, not the same. It obviates the "electronic" limitation of Senate bill 240, but it lacks the important provision of "general purpose." Thus, it appears that Florida law could also find computer crime in unlikely places such as wristwatches. The Florida law defines three categories of offenses: offenses against intellectual property, offenses against computer equipment and supplies, and offenses against computer users.[165]

Offenses against intellectual property include knowing and unauthorized modification, alteration, or destruction of programs, data, or supporting documentation, as well as the taking of computer-related documents which are trade secrets.[166] Presumably, this latter category would include the unauthorized taking of a copy of a secret program. Offenses against computer equipment include taking, injuring, or damaging the tangible objects associated with a computer system.[167] The heart of the section on offenses against computer users is the following paragraph:

> Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services, . . . which, in whole or part, is owned

---

[160]ARIZ. REV. STAT. ANN. § 13-2316 (1978).
[161]*Id.* § 13-1801.
[162]*Hearings*, *supra* note 6, at 136.
[163]FLA. STAT. §§ 815.01-.07 (Supp. 1979).
[164]*Id.* § 815.03(3).
[165]*Id.* §§ 815.04-.06.
[166]*Id.* § 815.04.
[167]*Id.* § 815.05.

> by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.[168]

In its attempt to define and address computer abuse and to address special computer-related questions which are not likely to be answered by existing law, the Florida statute is unquestionably the best of the three laws considered. Knowing and willful alteration of the program of another so that it will not run is a crime under Florida law. One need not argue the value of the damage done, the cost of correcting the damage, or whether the owner was deprived of control. The alteration can be prosecuted as an offense against intellectual property.

An ideal computer abuse bill should be general and flexible enough to lend itself to rapidly exploding computer technology and new uses to which computers might be put, yet narrow enough to exclude watches, traffic signals and pocket calculators. It should address those special questions that computers raise without unnecessarily infringing on areas already covered by existing legislation. Finally, it should specify exactly which acts constitute crimes under the law and which do not.

At least two approaches are possible. The first is to draft statutes which expand common law notions of property and asportation, at least in the case of computer-related items, to enable acts of computer abuse to be treated under existing penal statutes. The second alternative is to draft laws specifically creating new offenses related to computer abuse. The advantage of the first approach, of course, is that it takes advantage of existing law, law with which courts and attorneys have already had experience. The following is a suggested example of this type of statute: For purposes of application of any statute in which the taking of, or damage to, property is an essential element, property shall include computer programs, whether internal or external to, a computer. A computer program will have been asported or taken if an unauthorized copy is made, it being sufficient that the copy, if not reduced to tangible form, is embodied internal to a computer system, even though the owner of the program thus copied remains in possession and control of his original. If the value of such program asported is to be established, it shall be the commercial value of the program as established by expert witness.

As an example of model legislation embodying the second approach, this writer recommends the Florida statute slightly modified by using the ACM definitions throughout.[169]

---

[168] *Id* § 815.06.

[169] The ACM definitions are given in *Hearings*, *supra* note 6, at 54. The relevant portions of the Florida legislation are reprinted. *Id.* at 136-38.

IV. Indiana Law

A. The Case of John Thommen

A recent Indiana case[170] dealt with virtually all of the legal issues raised by computer abuse. The defendant, John Thommen, was convicted of theft, which the Indiana Code defines as "unauthorized control over property of another person, with intent to deprive the other person of any part of its value or use."[171]

John Thommen was a statistician in the Indiana Department of Mental Health. Because of the nature of his work, he was given one of a limited number of TSO (time-sharing option) terminals in use on the Indiana Central Data Processing Network. TSO terminals permit the user to modify programs he is running as well as receive data. Central Data Processing (CDP) ran two IBM 370/168 computers in tandem and served more than fifty state agencies, including the Bureau of Motor Vehicles, various licensing and registration boards, and the Department of Public Welfare.

Because so many different agencies used the same network, there was an operating systems program which was designed to prevent any user from obtaining access to any file or program to which his job did not entitle him. Because Thommen had a TSO terminal and was able to obtain the name of this systems program and the special program which enabled him to print a copy, he was able to modify the program to permit him to access any program or file of any kind anywhere on the system. Thommen kept an altered version of the security program in his own files. When he wanted to access files which the original security program would not have permitted him to have, he replaced that security program with his own, obtained the files or information he wanted, and then reinserted the correct security program into the system. Anyone checking the security program, except during those times when he had his own version in operation, would have found nothing amiss.

Thommen's duties for the Department of Mental Health included generating reports and creating statistical data. He had no programming responsibilities, and he certainly did not have authorization from his superiors to embark on a full-scale exploration of CDP. As

---

[170]State v. Thommen, No. 79-424B (Crim. Ct. Marion Co. Feb. 14, 1980).

[171]Ind. Code § 35-43-4-2(a) (Supp. 1979). Most of the information concerning the case of John Thommen was gained in a two hour interview on March 6, 1980, with Sgt. James Smith of the State Police Data Processing Section, who was the principal investigator on the Thommen case. Sgt. Smith also allowed the author to read in his office certain reports written as a result of his investigation. State Police regulations prevented the author from removing this material from Sgt. Smith's office or making copies. *See Statistician Convicted in Computer Case*, The Indianapolis Star, Feb. 14, 1980, at 26, col. 1.

a computer user in the Indiana CDP network, he had been assigned an identification code (ID) which identified him and his department, and which also permitted the system to keep track, to a limited extent, of how much he used the computer and what programs he used. The ID also served as the key in the security program to determine what files or programs he could legitimately access. Whenever Thommen's ID was used to "log on" to the system, CDP automatically made a record of it. There was, however, no means of confirming that it was Thommen personnally who was using that ID, or that Thommen at times was not actually doing computer work under someone else's ID. There was not even a way to determine which terminal was being used under Thommen's ID or where it was located. This, of course, presented a serious identification problem in trying to tie Thommen to any illegal computer uses. Anyone familiar with Thommen's ID and certain other easily accessible information could have been using the system as well as he.

Again, the fact that something was amiss was discovered completely by chance. Each user in the CDP network is assigned a support team, essentially a group of consultants. One member of a support team visiting the Department of Mental Health was helping Thommen with a problem with one of his statistical programs when the support team member happened to notice a "print-out" lying in plain view on Thommen's desk; the print-out, the consultant realized, was of a highly confidential security program to which even the consultant did not have access.

The consultant reported his discovery to his superior, who was equally surprised to find that Thommen had a copy of such a restricted program. They were not yet aware of the extent to which Thommen had actually compromised what security there was in their network or how much unauthorized use Thommen had made of files to which he supposedly had no access.

The State Police were called in to investigate the irregularities, although Thommen did not, at that time, realize that his activities were attracting attention. The investigation was conducted primarily by Sgt. James Smith of the Data Processing Division of the Indiana State Police. Compiling evidence took literally hundreds of hours of Sgt. Smith's time because he had to familiarize himself with the CDP system as well as print and sift through volumes of computer print-outs concerning terminal and computer usage involving Thommen's ID and other IDs used in the Department of Mental Health. The investigation was also complicated by the fact that CDP had no adequate method of keeping track of computer usage. Smith had to meticulously cull through piles of records to find what accesses had been made on Thommen's ID and what particular systems programs

or files were called during that access. If the program or file called had no relationship to Thommen's work, it was considered an unauthorized access. More than 3,700 such unauthorized accesses were found. Sgt. Smith estimated that Thommen was spending at least twenty percent of his working time dealing with material which was not related to his job functions with the Department of Mental Health. Sgt. Smith's investigation continued from May 27, 1978, until May 4, 1979, when CDP, alarmed at the potential consequences of Thommen's manipulations of their system, invalidated his access code. Denial of access to the computer alerted Thommen that he was under investigation. He was then able to destroy whatever "hard copy" evidence there may have been to link him with the abuses with which he was later formally charged. Any chance of determining exactly what modifications Thommen had made in the computer system, or what, if any, personal gain he had received from his efforts were lost.

The prosecutor seeking an indictment and later a conviction against Thommen was faced with important problems of evidence and procedure. In the first place, it was impossible to determine whether Thommen had used the computer to take money. Thommen had accessed a highly sensitive program in the Department of Public Welfare which was designed to make payments automatically to qualified individuals and services. He also had the capability to make the computer issue checks to fictitious accounts, an action almost impossible to detect with the audit procedures then in use.[172] The prosecutor tried to frame an indictment so that if theft of funds was discovered later, prosecution would not be barred by double jeopardy. This problem was solved by charging Thommen with theft of computer time, specifically, nine separate instances of unauthorized access to programs.[173]

There was the additional problem of tying Thommen to the unauthorized uses. All that was known initially was that someone somewhere, using Thommen's ID, was using the computer. There was no direct evidence that the person using Thommen's ID was

---

[172]*Cf. Fraud Scheme at SSA Office Nets $500,000*, COMPUTERWORLD, Mar. 3, 1980, at 1, col. 1 (computer fraud involving Social Security disability claims).

[173]One of these counts was based on playing computer games; the remainder were based on more substantial activities. Sgt. Smith reported receiving several phone calls from local industry complaining that the Thommen conviction might unduly frighten computer operators who had indulged in such relatively innocuous activities as game playing on the company computer. Sgt. Smith indicated that no prosecutions for such activity were planned and that the Thommen case was unusual because of the scope of the abuse involved. Interview with Sgt. James Smith, Indiana State Police Data Processing Section, in Indianapolis (Mar. 6, 1980) [hereinafter cited as Interview].

Thommen. Thommen solved this problem for the prosecution by admitting that he was the unauthorized user of the computer during the times in issue. He claimed, however, that he was merely sharpening his skills and that he had never been given any instructions as to what he could or could not do with the computer. If Thommen had not admitted he was the one who made improper use of the computer, it may have been impossible to convict him.

One of the most serious evidentiary problems was the highly technical nature of the evidence.[174] Persons who are not knowledgeable in computer use may find it hard to understand why, if Thommen could "call" certain files stored in the computer, he could not look at certain other files.[175] The swapping in and out of the computer's operating system of the program which allowed Thommen to read files to which he should not have had access was used to prove intent. Also relevant was Thommen's effort to hide what he was doing until he was finally confronted by the police.

The Indiana Criminal Code states: "A person who knowingly or intentionally exerts unauthorized control over property of another person, with intent to deprive the other person of any part of its value or use commits theft, a Class D felony."[176] Because Thommen did not have permission to access the files he dealt with or to engage in programming apart from his statistical analyses in conjunction with his job, his actions constituted unauthorized control over property of the State of Indiana.[177] A more difficult question was the value of what was taken. Because only nine of some 3,000 unauthorized accesses were in issue, most of the exhaustive analysis that Sgt. Smith had done to try to put a value on the total work time and computer usage devoted to non-work-related activities was held inadmissible. The prosecution did manage to convince the jury that something of value was taken.[178]

In his defense, Thommen argued that there were no explicit

---

[174]Even the judge commented that the testimony was so technical that he "had trouble following it." The Indianapolis Star, *supra* note 171, at 26.

[175]Could a public library restrict a patron to books on specific shelves? Could it prosecute him for looking at books on the forbidden shelves?

[176]IND. CODE § 35-43-4-2(a) (Supp. 1979).

[177]State v. Thommen, No. 79-424B (Crim. Ct. Marion Co. Feb. 14, 1980). Sgt. Smith indicated that neither the prosecution nor the defense seemed to have been aware of that section of the Indiana Code that defines "unauthorized." Interview, *supra* note 173. Unauthorized control is defined as control exerted, *inter alia*, "(1) without the other person's consent; (2) in a manner or to an extent other than that to which the other person has consented." IND. CODE § 35-43-4-1(b) (Supp. 1979).

[178]State v. Thommen, No. 79-424B (Crim. Ct. Marion Co. Feb. 14, 1980). Note that the statute in question does not require proof of a specific value, only that the object has some value. IND. CODE § 35-43-4-2 (Supp. 1979).

rules prohibiting his access to the files in question; that he did not deprive the State of anything;[179] and that what he did was job related because it sharpened his skills as a computer operator. Nevertheless, the jury found Thommen guilty on all nine counts.[180]

The implications of this case for Indiana's CDP, and other computer systems, are staggering. Apart from Thommen's legal guilt or innocence, this case demonstrated that the security of CDP, which serves virtually all State agencies and offices, was so weak that someone at one terminal in one department could compromise the entire system, read and alter programs and files throughout the system at will, and even cause large sums to be paid to himself in a manner that was all but undetectable. It showed that CDP had no adequate means to determine who was using its system, that there was no adequate billing procedure to determine the value of any work done on the system, and that there were no clear rules governing the conduct of those whose jobs gave them access to the system. There were no alarms that alerted authorities when a user accessed a particularly sensitive program, and no way to check whether any of the systems programs or files stored in the system had been altered. Sgt. Smith voiced a fear that Thommen may have put a "time bomb" into the system which will "explode" in months by sending him a check for $1 million.[181] At the present time, there is no way to detect the existence of that time bomb.[182]

---

[179]The CDP computer was, after all, running all of the time anyway. It could be argued that Thommen's use of the machine really took nothing away and caused the state no added expenses.

[180]State v. Thommen, No. 79-424B (Crim. Ct. Marion Co. Feb. 14, 1980).

[181]Interview, *supra* note 173.

[182]Needless to say, the State CDP has installed far stricter security checks in the system and taken other strong measures to prevent a repetition of the Thommen affair. The following recommendations came out of the Thommen trial and some have already been implemented:

1) There must be better communication between the users of the system and manufacturers of software for the system, that is, CDP. A more formal and reliable procedure must be established between CDP and the user for passing on vital information.

2) All terminal operators must be given a formal interview in which they are given a detailed description of their job and the scope of access they are to have within the system. They should be required to sign an agreement indicating that they have been given this knowledge and that they realize the penalties for refusing to abide by it.

3) There must be a better billing system for the network so that accurate records can be kept of how much use each department and user is making of the network, and for what purposes the computer is being used.

4) All areas of sensitive information must be protected from shared access.

5) CDP must closely monitor systems usage and notify appropriate authorities promptly when something happens that is suspect.

The *Thommen* case is undoubtedly one of the more complex and interesting instances of computer abuse in recent years. It is frightening to consider what Thommen could have done in the way of personal gain or damage to records which are vital to the government of Indiana. It is not known, however, how much he really did. He may even have performed a substantial service by alerting the State to the ease with which the CDP network on which it had become so dependent could be compromised. A future Thommen will find the work much more difficult; it is doubtful that he will find it impossible.

There are interesting questions which could have arisen in the Thommen case but did not; they could easily arise in a later case. First, if Thommen had not confessed, it may have been impossible to tie him to the unauthorized use of computer time. All that was known was that someone using Thommen's ID had done certain things. It was also known that Thommen had occasionally used someone else's ID; such a practice is not unknown in computer usage and there are sometimes good reasons for it. The computer had no means of tracing a use under Thommen's ID to Thommen's terminal.

Second, if Thommen had stored evidence in a small home computer linked to CDP computing by a telephone line, another problem would have been created. The evidence that could have been gleaned from use records available directly from CDP would have been entirely circumstantial and could not have linked Thommen directly to the abuses. Could CDP have "searched" Thommen's home computer without a search warrant sometime when Thommen was linked to the CDP machine; that is, could the State have used the same vehicle to read Thommen's computer files stored in his own computer at home that Thommen was using to read State files, or would a search warrant have been required?[183] The answers to these questions are not clear, but they are certain to arise in some future case.

---

6) All CDP users, such as the Department of Mental Health, must know and periodically review the rules of the computer network. When Thommen was compromising the network, many users did not have any idea what was or was not permitted, even according to law.

7) All CDP users must assume strict responsibility for monitoring the computer use of those who work for them. One reason that Thommen was able to do so much questionable work was that no one was checking on him to see what he was doing. It was purely by accident, and because Thommen was careless, that his unauthorized altering of the systems security program was detected. Interview, *supra* note 173.

There remains as well the question of what effect federal wire tap legislation, 18 U.S.C. §§ 2510-2520 (1970), might have on these issues. This question is beyond the scope of this Article.

[183]Associate Professor Henry Karlson of Indiana University School of Law—Indianapolis proposes as an alternative that an authorized copy be considered owned by the owner of the original from which the copy was made.

B. Recommendations

If Thommen's conviction is upheld on appeal under theories which are genuine tests of Indiana's criminal code, if CDP is careful to plug the huge gaps in security through which John Thommen wandered almost at will, if other computer users are also security conscious, and if new technology presents no problems beyond those covered in the current criminal code, then Indiana may not require special legislation dealing with computer crime. If, however, new legislation is called for, the author has made suggestions in the appendices to this Article.

The proposed statutory revisions in Appendix A build upon the current Indiana Code by adding certain computer-related concepts to the definition of property that may be subject to coversion. Appendix B, on the other hand, contains a new section that deals specifically with computer crime. John Thommen was convicted because the jury was convinced that he took "something of value," but the actual value was never shown. Someone who "practices" computer skills by printing a Snoopy calendar also takes something of value in the same sense that Thommen did. Under current law, both are equally subject to prosecution. Appendix B takes into account the special nature of computer abuses and classifies them appropriately.

Computer crime is the crime of the future that is rapidly becoming the crime of the present. Its limits are bounded only by the size and speed of the machines and the skill and imagination of those who use them to subvert the law. The *Thommen* case indicates the scope of the problem. The alternative to ignoring the problem is to leave both government and industry, as well as the general public, open to theft on a scale that dwarfs all previous forms of white collar crime and to losses that must become an intolerable burden for society to bear.

Appendix A

Proposed amendments to existing sections of the Indiana Criminal Code, IND. CODE tit. 35, (1976 & Supp. 1979), which might clarify certain issues involving computer crime include the items listed below. The additions are italicized.

In § 35-41-1-2: "Property" means anything of value; and includes, *but is not limited to*, a gain or advantage *or service* or anything that might reasonably be regarded as such by the beneficiary . . . .

Add to § 35-41-1-2: *The "value" of any property shall be its commercial value, reasonable retail value or cost of production, whichever is greatest.*

In § 35-43-4-1(a): As used in this chapter, "exert control over property" means to obtain, take, *copy, alter,* carry, drive . . . or extend a right to property. *If property is copied or altered, control is exerted through the act of copying or altering, and it is not required that the actor in such an instance exclude the property in question from the possession, control, or use of its owner. A copy or alteration need not be tangible if such copy or altered property may be reduced to tangible form.*

Add to the definition of "credit card" in § 35-43-5-1: *This definition shall be construed to include account numbers, project numbers, passwords or similar signs, symbols or devices by which the holder gains access to goods or services or other property, including, but not limited to, the use of computer services, computer programs, files or data, in any medium.*

With the above proposed clarifications and additions, the following sections may be used to combat computer crime:

35-43-1-2 (criminal mischief)
35-43-4-2 (theft)
35-43-4-3 (criminal conversion)
35-43-5-4 (fraud)

Other sections such as 35-43-2-2 (criminal trespass) and 35-44-3-4 (tampering) may also be applicable in certain situations.

Appendix B

The following is offered as a possible additional section to the Indiana Criminal Code to deal specificaliy with various forms of computer abuse. It is modeled after the Florida statute.

As used in this section, unless the context clearly indicates otherwise:

"Intellectual property" means data including programs.

"Computer program" means an ordered set of data representing coded instruction or statements that when executed by a computer cause the computer to process data.

"Computer" means an internally-programmed, general purpose, automatic device that performs data processing.

"Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

"Computer system" means a set of related, connected or unconnected, computer equipment, devices, or computer software.

"Computer network" means a set of related, remotely connected devices and communications facilities including more than one computer system with capability to transmit data among them through communications channels.

"Computer system services" means providing a computer system or computer network to perform useful work.

"Property" means anything of value as defined in section 35-41-1-1, and includes, but is not limited to, financial instruments, information, including electronically reproduced data and computer software and programs in either machine or human readable form, or any other tangible or intangible item of value.

"Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

"Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resource of a computer, computer system, or computer network.

The "value" of property is its commercial value, reasonable retail value, or cost of production, whichever is greatest. The assessment of "value of damage" to property is determined by the cost of restoring the property to its condition immediately prior to being damaged.

Offenses against intellectual property—

1) Whoever willfully, knowingly and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

2) Whoever willfully, knowingly and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

3) Whoever willfully, knowingly and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret, or is confidential as provided by law, residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

4) An offense against intellectual property is a Class B misdemeanor. However, the offense is a Class A misdemeanor if the value of the property acted upon is at least two hundred fifty dollars ($250) but less than two thousand five hundred dollars ($2500), and a Class D felony if (i) the value of the property acted upon is at least two thousand five hundred dollars ($2500), (ii) the damage causes a substantial interruption or impairment of utility service rendered to the public, (iii) the owner of the property is a bank or financial institution, or (iv) the offense involves property which is confidential as a matter of law.

Offenses against computer equipment or supplies—

1) Whoever willfully, knowingly and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system or computer network commits an offense against computer equipment or supplies.

2) An offense against computer equipment or supplies is a Class B misdemeanor. However, this offense is a Class A misdemeanor if the cost of restoring the equipment or supplies to their condition immediately prior to modification is at least two hundred fifty dollars ($250) but less than two thousand five hundred dollars ($2500), and a Class D felony if (i) the cost of restoration is at least two thousand five hundred dollars ($2500), (ii) the modification causes a substantial interruption or impairment of utility service rendered to the public, (iii) the equipment or supplies belong to a financial institution or bank, or health care facility, or (iv) the modification poses an unreasonable danger to other property or to human life.

3) Whoever willfully, knowingly and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly and without authorization destroys, injures or damages any computer, computer system, or computer network commits an offense against computer equipment or supplies.

4) The penalties for the offense described in (3) shall be the same as those described in (4) of the section concerning offenses against intellectual property.

Offenses against computer users—

1) Whoever willfully, knowingly and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly and without authorization denies or causes to be denied computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.

2) An offense against computer users is a Class B misdemeanor. However, this offense is a Class D felony if (i) the act causes a substantial interruption or impairment of utility service rendered to the public, (ii) interferes with the operation of a bank, financial institution, or health care facility, or (iii) involves an intent to devise or execute any scheme to obtain by fraud property the value of which exceeds one thousand dollars ($1000).

Chapter not exclusive—Nothing in this chapter shall be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter.

If any provision of this act or the application thereof to any person or circumstance is held invalid, it is the legislative intent that the invalidity shall not affect other provisions or applications of the act which can be given effect without the invalid provisions or applications, and to this end the provisions of this act are declared severable.