UIC John Marshall Journal of Information Technology & Privacy Law

Volume 4
Issue 1 *Computer/Law Journal - Summer 1983*

Article 8

Summer 1983

Addressing Computer Crime Legislation: Progress and Regress, 4 Computer L.J. 195 (1983)

Pamela Gonzalez

Recommended Citation

Pamela Gonzalez, Addressing Computer Crime Legislation: Progress and Regress, 4 Computer L.J. 195 (1983)

ADDRESSING COMPUTER CRIME LEGISLATION: PROGRESS AND REGRESS

Losses resulting from computer-related crimes[1] are estimated to be between $100 and $300 million annually in the United States.[2] For example, a large insurance company was recently the victim of "electronic vandalism." After being fired, an irate woman strolled through the computer room with a powerful electromagnet and caused an estimated $10 million in damages to the system.[3] It is estimated that fewer than one percent of computer-related crimes are ever detected.[4] Until recently, concerted efforts to prosecute such crimes have been haphazard and ineffective,[5] in part due to the difficulty in establishing a criminal offense under existing federal and state statutes.[6]

This Note discusses the deficiencies in existing legislation relating to computer crimes and presents an analytical framework to evaluate legislation relating to computer abuse. Special focus is placed on the statutory creation of a crime against intellectual property and computer users under the Florida Computer Crimes Act.[7]

I. PROBLEMS PECULIAR TO COMPUTER CRIME

Before discussing deficiencies in existing criminal statutes, it is necessary to review the most common methods of perpetrating com-

[1] The definition of a computer-related abuse and its incidence have been the subject of much debate. *See, e.g.*, Parker, *Computer Abuse Research Update*, 2 COMPUTER/L.J. 329 (1980); Taber, *A Survey of Computer Crime Studies*, 2 COMPUTER/L.J. 275 (1980). *See also infra* notes 8-9 and accompanying text.

[2] L.A. Daily J., May 5, 1980, at 3, col. 2. The estimated average "take" per crime is $430,000. *See* Rivlin, *Computer Crime*, 10 STUDENT LAW. 15-16 (1980).

[3] *Id.* at 17, comment (*A Gallimaufry of Computer Scams*).

[4] A. BEQUAI, COMPUTER CRIME xiii (1978).

[5] *See generally* Coughran, *Prosecution of Computer Abuse*, 1 CRIM. JUST. J. 397 (1978); Ingraham, *On Charging Computer Crime*, 2 COMPUTER/L.J. 429 (1980).

[6] Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMPUTER/L.J. 353, 373 (1980). *See* Becker, *The Trial of a Computer Crime*, 2 COMPUTER/L.J. 441, 445-49 (1980).

[7] FLA. STAT. ANN. §§ 815.01-.07 (West Supp. 1982).

puter crimes and to discuss a definitional framework for analyzing computer crime.

A. An Analytic Framework

There is presently no agreement among commentators as to what constitutes a "computer crime," and consequently, a universal definition of computer crime is notably absent from the vocabulary of current literature. In studies sponsored by the Stanford Research Institute, Donn Parker carefully chose the term "computer abuse" rather than "computer crime" to describe his work[8] because his studies analyze some abuses that do not involve criminal activities as a court of law might define such behavior.[9] But, in response to Parker's terminology, John Taber points out that such inconsistent treatment causes confusion because many people interpret "abuse" to mean crime.[10]

A more extreme definitional position is that computer crime does not exist as a separate type of crime. This view is advanced by Donald Ingraham, a Deputy District Attorney in California, who believes that computer crime is really nothing more than a variation on an old theme and that there is only crime by computer, not computer crime.[11] From Ingraham's perspective, unauthorized use of processing time on a computer is more properly classified as theft; manipulation of computerized data to cover up the pilferage of inventory is more properly classified as embezzlement, and "snooping" through computer files is more properly classified as invasion of privacy.[12] Some authors, therefore, discuss the subject in terms of "computer-assisted" crime rather than in terms of computer crime or abuse.[13]

Computer abuse can be placed in one of five categories of currently recognized crime: financial crime, informational crime, theft

[8] *See* Parker, *supra* note 1, at 333-35. Parker heads the Stanford Research Institute's program on the Study of Computer Abuses, a program sponsored by the National Science Foundation.

[9] The Fourth Circuit has adopted the phrase "computer abuse" as a term of art. *See* United States v. Jones, 553 F.2d 351, 353 n.6 (4th Cir.), *cert. denied*, 451 U.S. 968 (1977).

[10] *See* Taber, *supra* note 1. John Taber is a systems programmer and an author of articles on computer crime. For purposes of this Note, the term "computer abuse" will be used because it is the most inclusive. *See also* Kling, *Computer Abuse and Computer Crime as Organizational Activities*, 2 COMPUTER/L.J. 403, 407-08 (1980).

[11] Ingraham, *supra* note 5, at 430-37. Ingraham is a former chairman of the Computer Abuse Subsection of the American Bar Association.

[12] *Id.*

[13] Schøjlberg, *Computer-Assisted Crime in Scandanavia*, 2 COMPUTER/L.J. 457 (1980).

of property, theft of services, and vandalism. A financial crime is the taking of funds via computer, for example, executing the theft through a system with a computer payroll. The informational crime, one of the least detected and most expensive types of computer crime, involves the acquisition of valuable information via computer, information such as a company's mailing lists. A theft of property is simply the taking of computer merchandise for personal sale or use. A theft of services is the unauthorized use of a computer, for example, use of a company's computer for personal, nonofficial use. Finally, vandalism is intentional damage to a computer or computer system, either by physical destruction or by altering the system.[14]

Some computer abuse fits more easily into our traditional criminal statutory scheme, such as theft of physical computer property and vandalism. Other types of abuse, such as the taking of information or services, are more difficult to analyze in traditional terms. The above categorization is consonant with Ingraham's notion that the computer is merely a tool to perpetrate age-old crimes or abuses.[15]

Another commentator on computer abuse, Susan Nycum, has suggested a method for analyzing computer software abuses according to the *manner* of misappropriation[16]:

(1) misappropriation of software through the use of a remote terminal[17];

(2) misappropriation of software through *direct* access to a computer center or software storage facility[18];

  (a) unauthorized or fraudulent access by unprivileged users;

  (b) unauthorized or fraudulent access to software by an employee or former employee;

(3) obliteration or bugging of software by inflicting physical damage[19]; and

[14] Tunick, *Computer Law: An Overview*, 13 LOY. L.A.L. REV. 315, 328 (1980).

[15] *See supra* note 5.

[16] Nycum, *The Criminal Law Aspects of Computer Abuse*, 5 RUT. J. COMPUTERS & LAW 271, 276-94 (1976). Susan Nycum is a legal consultant to the Stanford Research Institute's Study of Computer Abuses for the National Science Foundation.

[17] *Id.* at 276-87. An individual who misappropriates software by using a remote terminal could be prosecuted under a larceny or trade secret statute, and, if a credit card is used to perpetrate the offense, an individual could be prosecuted under a false pretenses statute. *Id.*

[18] *Id.* at 287-91. This form of abuse is similar to the statutory crimes of vandalism or criminal mischief. Interference with computer use is difficult to prosecute unless there is physical damage to the computer. Some prosecutions in this area have been successful through use of criminal tampering or trespass statutes.

[19] D. PARKER, S. NYCUM & S. OURA, COMPUTER ABUSE 79 (1973). As of 1978, over two million people were operating approximately ninety thousand computers. *See*

(4) miscellaneous abuses, such as, credit card abuse, for example. This analysis draws attention to how the computer abuse is perpetrated and away from the resultant harm. It also reflects the fact that there are five key points in a computer system through which one can gain access to information: input, programming, the central processing unit, output, and remote transmission.[20]

In summary, although recognition of the type of harm caused by the computer crime is important to the analysis of the computer abuse problem, focus on how the abuse is committed is extremely important.[21] It is essential that the courts and legislators realize that the uniqueness of computer abuse lies in the many ways of gaining access to the computer. Computer abuse can occur in unobtrusive ways, such as through fraudulent access or bugging of software. Furthermore, detection is especially difficult since the unauthorized user often is someone very familiar with the computer system.[22]

B. THE DEVELOPMENT AND USE OF CONVENTIONAL THEFT LAWS

Criminal law has traditionally placed great emphasis on tangible thefts, yet many computer thefts occur without damaging the computer or removing property.[23] The lack of criminal statutes specifically addressing computer theft may jeopardize prosecution of such computer crimes.[24]

1. *The History of the Law of Theft*

The history of the law of theft illuminates some of the reasons why traditional criminal statutes, such as larceny, have been inadequate in prosecuting computer abuses. Generally, the entire law of theft is a product of the eighteenth and nineteenth centuries.[25] By the middle of the nineteenth century, the laws of theft even covered stealing a piece of paper,[26] though similar property interests, such

generally A. BEQUAI, *supra* note 4, at 4, 19-24 (discussing the need for personnel and physical security).

[20] Roddy, *The Federal Computer Systems Protection Act*, 7 RUTGERS J. COMPUTER TECH. & L. 343, 347 (1980). *See* Lahore, *Computers and the Law: The Protection of Intellectual Property*, 9 FED. L. REV. 15 (1978).

[21] Sokolik, *supra* note 6, at 364-65.

[22] *Id.* at 365-66. *See* A. BEQUAI, *supra* note 4, at 28.

[23] Volgyes, *The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the Art Review*, 2 COMPUTER/L.J. 385, 398 (1980).

[24] *See* Ingraham, *supra* note 5.

[25] J. HALL, THEFT, LAW AND SOCIETY 34-36 (1935).

[26] Regina v. Perry, 1 Carr & Kir. 725 (1848); J.F. STEPHENS, COMMENTARIES ON THE LAWS OF ENGLAND 75 (1950).

as choses in action, realty, and electricity,[27] had previously been considered objects incapable of being stolen.

Before the 1850's, the most significant impact on the law of theft was the *Carrier's Case* in 1473.[28] In this case, the court recognized the ability of a bailee to "trespass" on the goods of his bailor. Until that time, the court had found that, for legal purposes, a bailee was considered to be "in possession" of the bailor's goods, and therefore was incapable of stealing from himself. By refinement of the *Carrier's Case*, a series of acts that had been civil wrongs were admitted into the law of larceny.[29] With the advent of large scale marketing and purchase of goods, safeguards against fraud became necessary.[30] The last twenty years of the eighteenth century produced the most rapid and extensive growth of the entire law of theft. This growth of the theft doctrine survived in American courts. An early case, *Missouri v. McLaughlin*,[31] permitted a voter's referendum to be the object of theft, thus extending the law of theft to cover written instruments. The court, however, qualified its decision by stating that the referendum contained valuable signatures.

The historical development of the crime of theft reflects the economic flux of the nation's history. Change in the law has been relatively recent and tends to follow rather than lead economic development within the country. Steadfastly implanted in the law of theft is the notion that property capable of being stolen must be tangible and that such property must physically change possession.[32]

It becomes difficult, therefore, to apply the common law and statutes based upon the law of theft when faced with the unique elements of computer abuse. For example, to be guilty of the crime of "stealing," according to Sir James Fitzjames Stephen, one must "without the consent of the owner, fraudulently and without claim of right made in good faith, tak[e] and carr[y] away anything capable of being stolen with intent, at the time of such taking, permanently to deprive the owner thereof. . . ."[33] Included in this definition is an explanation of things capable of being stolen, that is, "[e]verything which has value and is the property of any person, and if adhering to the realty then after severance therefrom, is capa-

[27] A. WILSHIRE, HARRIS' CRIMINAL LAW 190 (14th ed. 1926).

[28] J. HALL, *supra* note 25, at 315-46.

[29] *Id.* at 6.

[30] *Id.* at 24-33.

[31] 3 H.C.L. 144 (1919).

[32] G. WILLIAMS, TEXTBOOK OF CRIMINAL LAW 676-89 (1978).

[33] J. STEPHEN, A DIGEST OF CRIMINAL LAW 302 (7th ed. 1950). Sir James Fitzjames Stephen was a notable British author and attorney who specialized in criminal law. His books contain some of the first coherent definitions in criminal law.

ble of being stolen. . . ."[34] Further, Stephen states that "[i]f the thing taken and carried away is for the first time made capable of being stolen by the act of taking and carrying away, and if the taking and carrying away is one continuous act, such taking and carrying away is not stealing unless it is provided that it should be."[35] Therefore, under Stephen's analysis, if nothing is physically removed from the computer premises, or if the computer item is not actually taken and carried away from the premises,[36] such as in the case of stealing the *use* of a computer terminal, then this law is difficult to apply.

The tangibility issue was addressed in *Ward v. Superior Court*.[37] The court found that the defendant had not stolen an "article" within the meaning of the penal code because implicit in the definition of the article is that it must be something tangible. The court found that electronic impulses are not tangible.[38]

Valuation of the item is necessary in order to distinguish a felony offense from a misdemeanor offense, and consequently, to determine the respective penalties. If some piece of the computer program or system is actually stolen, valuation of what was stolen is difficult. Is it the price of the paper on which the program was written, or is it the value of the bit of information to the company or the owner of the program?[39]

A recent case illustrates the problem of inadequate criminal statutes. In *United States v. Siedlitz*,[40] an individual used a telephone to gain access to a former employer's computer and thereby obtained a valuable and confidential program. United States attorneys in Maryland and Virginia, attempting to prosecute the theft, encountered difficulty in using the federal statute prohibiting interstate transportation of stolen property. Not only was the statute unclear about whether the electronic impulses were property within the requirements of the statute, but furthermore, the movement of magnetic impulses from the victim's computer to the defendant's computer did not satisfy the traditional interpretation of "stealing"

[34] *Id.* at 306.

[35] *Id.* at 309.

[36] A. BEQUAI, *supra* note 4, at 28-29.

[37] Ward v. Superior Ct., 3 Computer L. Serv. Rep. (Callaghan) 206 (Cal. Sup. Ct. 1972).

[38] *Id.* at 208.

[39] The Fifth Circuit has rejected the argument that a stolen computer program has ascertainable value only as paper. *See* Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967).

[40] 589 F.2d 152 (4th Cir. 1978).

or "taking" of property as required by the statute.[41] Although Siedlitz was acquitted of the charge under the statute, he was convicted of wire fraud for using interstate phone signals in the fraud. *Siedlitz* demonstrates the complications that exist both in determining if a "taking" has occurred[42] and also in determining if the object of theft[43] can be classified as "property."

2. *Use of Non-Theft Statutes and Statutes Modeled Upon Traditional Crimes*

Other federal and state criminal statutes, including embezzlement,[44] invasion of privacy,[45] trade secret,[46] copyright,[47] and surprisingly, mail fraud laws,[48] have been used to prosecute computer crimes. Numerous problems exist in applying these criminal statutes to computer crimes. Shortcomings exist in these laws because there are gaps in their applicability to computer crimes and because some are subject to specific defenses. For example, in cases of embezzlement, if no property or money is converted, the criminal charge cannot be maintained.[49] Similarly, a trade secret theft charge is subject to the defense of "unprotected disclosure" if the computer trade secret owner failed to take reasonable precautions to protect the secrecy of the thing allegedly stolen.[50] The applicability of this defense is particularly appropriate in computer situations since often many employees are privy to the computer and its programs.

Some prosecutors and judges, who have specific computer crime statutes at their disposal, are reluctant to apply them to computer

[41] A. Bequai, *supra* note 4, at 39.

[42] Roddy, *supra* note 20.

[43] Sokolik, *supra* note 6, at 376.

[44] A. Bequai, *supra* note 4, at 31.

[45] For a list of federal and state privacy legislation passed as of 1977, see Nycum, *Legal Problems of Computer Abuse*, 1977 Wash. U.L.Q. 527, 533 nn.11 & 12. *See also* Tunick, *supra* note 14, at 335 (discussing common law and statutory privacy law in a computer crime context).

[46] *See* 18 U.S.C. § 1905 (1976) (theft of trade secrets by federal employees); Stamicarbon, N.V. v. American Cyanamid Co., 506 F.2d 532, 540 n.11 (2d Cir. 1974) (complete list of state trade secret statutes).

[47] 17 U.S.C. § 506 (1976) (federal copyright law). *See generally* Lahore, *supra* note 16 (discussing copyright problems with computer programs); *see also* Tunick, *supra* note 14, at 345 (using copyright laws for protection of computer software is an area of considerable dispute).

[48] 18 U.S.C. § 1341 (1952) (federal mail fraud statute); 18 U.S.C. § 1343 (1952) (wire fraud statute).

[49] *See supra* note 27 and accompanying text.

[50] Hedden, *Intellectual Property*, 6 Golden Gate U.L. Rev. 679, 688 (1975); *see supra* note 12 and accompanying text.

abuses because the statutes are simply variations on larceny or damage to property statutes.[51] Absent the determination of the value of stolen or damaged software, or absent evidence of the computer abuser's fraudulent intent, criminal prosecutions under many state computer crime statutes are cumbersome, if not impossible to implement.[52] As discussed above,[53] these computer crime statutes are applicable only if the property is damaged or taken and a value is placed on the damage or loss. For example, Virginia's computer crime statute explicitly describes computer services or data programs as items capable of being stolen, and therefore puts computer theft within the purview of the general larceny statute.[54]

II. BEYOND THE USE OF CONVENTIONAL CRIMINAL CONCEPTS: COMPUTER CRIME ACTS

Federal and state legislators have attempted to incorporate categories of computer abuses into computer crime acts. Use of these acts is an alternative to prosecuting computer abuse under conventional criminal statutes. For example, some statutes have criminalized many aspects of computer abuse such as theft of telecommunication services.[55]

A. Legislative Efforts to Deal With Computer Abuse

One of the forerunners of computer crime legislation was Senate Bill 1766, the Federal Computer Systems Protection Act of 1977.[56] Two years later, Senator Abraham Ribicoff sponsored Senate Bill 240,[57] which was virtually identical to its predecessor. Senate Bill 240 set forth penalties for using computers to defraud and steal from the United States government, financial institutions and other entities related to interstate commerce. It contained a broad definition of "computer" and a definition of property that included in-

[51] *See infra* note 54 and accompanying text.

[52] *See infra* note 60 and accompanying text.

[53] *See supra* notes 33-35 and accompanying text.

[54] VA. CODE §§ 18.2-98.1 (Supp. 1981).

[55] For a complete listing, see generally Lautsch, *Digest and Analysis of State Legislation Relating to Computer Technology*, 20 JURIMETRICS J. 201 (Spring 1980).

[56] S. 1766 was introduced by Senator Abraham Ribicoff in the Ninety-fifth Congress but was not reported out of the Judiciary Committee before the end of the second session. S. 1766, 95th Cong., 2d Sess., 123 CONG. REC. 21,023-21,025 (daily ed. June 27, 1977).

[57] S. 240, 96th Cong., 1st Sess. (1979). S. 240, the Federal Computer Systems Protection Act of 1979, was introduced in January 1979 (125 CONG. REC. 1190-1201 (daily ed. Jan. 25, 1979)) and amended in November 1979 (125 CONG. REC. S. 15901-15902 (November 5, 1979)).

tangibles.[58] Thus, under Senate Bill 240, an individual who damages a computer intentionally and without authorization would have received a $50,000 fine and five years imprisonment.[59] This bill was defeated because it was overbroad (as in the definition of property) and because it was difficult to apply it to intangible property.[60] Another bill, sponsored by Representative Nelson, who also authored the Florida Computer Crimes Act,[61] is presently pending before the House Judiciary Committee.[62]

Many states have passed bills modeled after Senate Bill 240. Such statutes contain two basic provisions. One provision penalizes any scheme to defraud by means of false or fraudulent pretenses through altering or accessing a computer, and a second provision penalizes damaging, destroying, or unauthorized accessing of any computer system. All such statutes contain either a "willful" or "knowing" mens rea requirement.[63]

The major difference among state computer statutes is the classification of a violation as a felony or misdemeanor and the corresponding penalty. Most state computer crime statutes classify the crime according to the value of the property stolen or damaged,[64] as in most larceny statutes. Depending upon the wording of the statute, the same valuation problems that arise when employing conventional criminal statutes to computer crime may arise even in those states with specific computer crime provisions.[65]

Several states with computer crime statutes criminalize the use of a computer to defraud or deceive by means of false pretenses, regardless of whether the victim incurred a monetary loss.[66] Two states, Arizona and Florida, have enacted statutes that establish

[58] S. 240, 96th Cong., 1st Sess. (1979) at p. 4, lines 8-13, 21-25, 51-52.

[59] *See* Bigelow, *Where Do We Stand on Computer Crime Law?*, 6 COMPUTER L. & TAX REP. 3.

[60] For criticism of S. 240, see Becker, *Trial of a Computer Crime in the United States*, 131 NEW.L.J. 908; Sokolik, *supra* note 6, at 380; Comment, *Computer Crime, Senate Bill S. 240*, 10 MEM. ST. U.L. REV. 660 (1980).

[61] *See supra* note 7 and accompanying text.

[62] H.R. REP. NO. 3970, 97th Cong., 1st Sess. 3141 (1981); *see Federal Computer Crime Legislation: Tilting at Windmills*, 1 THE SCOTT REPORT, Nov. 1981, at 14 (for analysis and comment on H.R. 3970).

[63] Arizona, California, Colorado, Florida, Illinois, New Mexico, North Carolina, Michigan, Rhode Island, and Utah all currently have some version of a computer crime statute. *See* Lautsch, *supra* note 55, at 212.

[64] COLO. REV. STAT. § 18-5.5-102(3) (Supp. 1980); ILL. ANN. STAT. ch. 38, § 16-9(3)(1) (Smith-Hurd Supp. 1981-1982); MICH. STAT. ANN. § 28.529(7) (Callaghan 1980); N.M. STAT. ANN. §§ 30-16A-3(B)(1)-3(B)(3) (Supp. 1981); UTAH CODE ANN. §§ 76-6-703(1)-703(4) (Supp. 1979).

[65] *See supra* notes 34-36 and accompanying text.

[66] ARIZ. REV. STAT. ANN. § 13-2316(A) (Supp. 1978); CAL. PENAL CODE § 502(d)

penalties according to the type of computer misappropriation rather than according to the value of the loss.[67] Computer crime statutes in Rhode Island and California do not differentiate penalties on either basis. Instead these statutes provide uniform penalties for any transgression falling within their ambit.[68] Some statutes require that a computer program be stored in a computer system before it can be the subject of unauthorized use, alteration, damage, or destruction.[69] Such provisions provide a loophole for the computer thief who steals a program not yet within the computer system.

The recent case of *New York v. Weg*[70] illustrates how computer crime statutes can be ineffective if they are too narrowly constructed. In *Weg*, the judge dismissed the theft of services charge against a computer systems manager employed by the New York Board of Education, who used the school computers to trace the genealogy of horses and to create a handicapping system for betting. The court found that Weg had not stolen computer time because his supervisor had given him general access to the computer. If Weg had plugged into a public computer without permission and was trying to avoid payment, his acts may have fallen within the purview of the statute. The court also noted that though the statute regulates theft of services from commercial ventures, the Board of Education is a noncommercial entity.

B. A Responsive Statutory Approach: Focus on the Abuse

The most innovative approach to the computer abuse problem is the Florida Computer Crimes Act.[71] It creates two new classifications of computer offenses: an offense against intellectual property and an offense against the authorized computer user. The first classification provides that whoever willfully, knowingly, and without authorization, modifies or destroys data, programs, or supporting documentation, internal or external to a computer, is guilty of a felony against intellectual property.[72] The second offense holds an individual liable for a felony if he, without authorization, denies an

(West Supp. 1981); Fla. Stat. Ann. § 815.04(4)(b) (West Supp. 1979); N.M. Stat. Ann. § 30-16A-3(A) (Supp. 1981); R.I. Gen. Laws § 11-52-4 (1979).

[67] Fla. Stat. Ann. §§ 815.04(4)(a), (b), 815.06(2)(a), (b) (West Supp. 1979); Ariz. Rev. Stat. Ann. § 13-2316(A), (B) (1978).

[68] R.I. Gen. Laws § 11-52-4 (1979); Cal. Penal Code § 502(b) (West Supp. 1981).

[69] *E.g.*, Colo. Rev. Stat. § 18-5.5-102(2) (Supp. 1981).

[70] No. 2329 (N.Y. Sup. Ct.) (April 12, 1982).

[71] Fla. Stat. Ann. §§ 815.01-815.07 (West Supp. 1981).

[72] *Id.* § 815.04.

authorized user access to computer system services.[73] This statute distinguishes misdemeanor and felony crimes on the basis of whether the offense involves damage, destruction or fraud, whether the offense results in interruption of government operation of public services, and whether the amount of damage to the computer or computer system falls within a specific range.[74]

Because it does not index the degree of the criminal charge exclusively to the amount of damage to the computer system, this statute goes beyond the traditional constraints of larceny or embezzlement statutes. The Florida statute recognizes computer abuse as a separate criminal activity with a range of degrees and penalties. By penalizing many types of computer abuses, such as unauthorized accessing, the statute shifts the focus away from the harm, the tangibility of the item, or the possession characteristics inherent in the elements of conventional theft laws.

Admittedly, the statute might be considered overly inclusive, in which case, prosecutorial discretion and possibly abuse will play a greater role. But prosecutional abuse is not likely to occur due to problems prosecutors have had in the past with respect to the amount of time required to investigate and prepare for a computer abuse case and to the lack of statutes with which to prosecute the computer abuser effectively.[75]

Florida's statute incorporates the best of both worlds. It retains the traditional criminal provisions for offenses against computer equipment or supplies.[76] It also includes provisions that protect intellectual property from modification, destruction, or disclosure[77] and provisions that protect the individuals who are entitled to access from unauthorized interference with their right to use. Depending on the nature of the offense, the Florida statute allows prosecution under traditional common law and statutory property analysis or for tampering with the computer or denying access to an authorized user. No other computer crime statute is more comprehensive.

Though the Arizona and California statutes, like the Florida statute, penalize unauthorized access to a computer or computer system, these statutes require proof of fraudulent intent or of a

[73] *Id.* § 815.06.

[74] *See* Sokolik, *supra* note 6, at 382 (summary of Florida's computer crime statute).

[75] Rivlin, *supra* note 2, at 18. *See also* A. BEQUAI, *supra* note 4, at 43-93 (examines inadequacies of procedural, investigatory, and legislative processes in dealing with computer crime).

[76] FLA. STAT. ANN. § 815.05 (West Supp. 1981).

[77] *Id.* § 815.04.

scheme to defraud.[78] If there is no such proof, the Arizona statute provides for a lesser penalty, while the California statute requires that the unauthorized access be malicious.[79]

Florida's statute is not flawless. For example, the statute's language may be used to convict an individual of a felony for stealing a digital watch with a built-in calendar or for using a computer to print a Snoopy calendar.[80] If the law focuses on the occurrence of the abuse, rather than on the degree of harm, then a felony prosecution in either case is entirely possible.

III. CONCLUSION

Present laws are inadequate to combat computer abuse. The computer age has opened doors to permit an array of criminal activity never before contemplated. New legislation is needed to avoid fitting a new type of misdeed into the all-purpose coat of the conventional cloth. In distinguishing felonies from misdemeanors, computer crime legislation should focus on the abusive acts of the computer criminal rather than on the amount of damage to the computer system.

Pamela Gonzalez

[78] ARIZ. REV. STAT. ANN. § 13-2316(A) (1978); CAL. PENAL CODE § 502(b) (West Supp. 1981); FLA. STAT. ANN. § 815.06 (West Supp. 1981).

[79] CAL. PENAL CODE § 502(c) (West Supp. 1981).

[80] *See* Bigelow, *supra* note 59, at 3-4. *See also* Rivlin, *supra* note 2, at 36.