
Amalia M. Wagner

Follow this and additional works at: https://digitalcommons.law.buffalo.edu/buffalolawreview

Part of the Communications Law Commons, Computer Law Commons, Criminal Law Commons, and the Intellectual Property Law Commons

Recommended Citation
Available at: https://digitalcommons.law.buffalo.edu/buffalolawreview/vol33/iss3/8
COMMENTS


INTRODUCTION

DURING the summer of 1983, the FBI identified several young computer hobbyists in the Milwaukee area who used their home computers and telephone equipment to break into business, medical, and government computer systems around the nation. The youths insisted that they did not intend to destroy or alter any information stored in these computers, and no charges were filed against them. In a similar case in October, 1983, FBI agents raided the homes of four California teenagers, confiscating computers, peripheral equipment, printouts, and other information which linked them to the unauthorized entry of General Telephone and Electronics’ Telenet. Unlike the firms and agen-


For a description of the methods used by these youths to enter the computer systems, see Clark, Computer Pirates, Buffalo News, Jan. 27, 1984, at C-7, col. 1.

2. Marbach, supra note 1, at 46.


4. Id.

5. Such equipment included modems (modulator-demodulators) (inexpensive devices which allow computers to transmit data over phone lines), Marbach, supra note 1, at 43 and printers which make copies of data and programs stored in a computer. See generally P. Coburn, P. Kelman, N. Roberts, T. Snyder, D. Watt & C. Weiner, Practical Guide to Computers in Education (1982) [hereinafter cited as Computers in Education].

6. Telenet is a powerful data-base network owned by GTE. It connects more than 1200 computers over telephone lines and has 150,000 authorized users who pay a fee for their subscription. Marbach, supra note 1, at 44. Other networks include LEXIS, a data-
cies in the Milwaukee incident, GTE insisted that it would "pursue all available legal recourse, including criminal prosecution." In November, 1983, a UCLA science student was arrested and charged with using his home computer to break into a multinational Defense Department computer system. He was jailed, pending arraignment, on charges of maliciously accessing a computer system, theft, and receiving stolen property.

The escalating severity of the official responses to these three cases is indicative of the escalating pressure on business, law enforcement agencies, and legislatures to resolve the increasingly serious and multi-faceted problems of computer crime. Many difficult issues are involved: whether laws regarding privacy must be recast in light of new technical developments; whether the new technology warrants the creation of a new category of proscribed behaviors; and whether and when civil versus criminal sanctions will be more effective. This Comment explores the aspects of those issues which relate to possible legislative approaches to these problems.

The Comment presents a brief outline of computer development and use and discusses some controversies surrounding the issues mentioned above, especially those concerning the definition of the term "computer crime" itself. Varying approaches to legislation which these different definitions engender are surveyed, including federal and state responses, with an emphasis on action taken by the New York state legislature. Existing New York State legislation is shown to be clearly inadequate to deal with some special considerations presented by computer-related crime, while wholesale creation of entirely new statutes is shown to be undesir-

7. Teen Computer Snoops, supra note 3, at A2, col. 3. Note, however, that no charges have been filed against the Irvine, California, students since the FBI raid in October, 1983. Computer Crime a Hot Subject in Schools, Buffalo News, Dec. 5, 1983, at A-11, col. 1. CAL PENAL CODE § 502(b) (West Supp. 1984) requires intent to defraud or "malicious intent to access" a computer system. This provision would make prosecution of the boys difficult, since the requisite intent evidently was absent.


9. See CAL PENAL CODE § 502(e) (West Supp. 1984). This offense carries a punishment of up to three years of imprisonment and a fine of up to $10,000.
able. This Comment concludes that the most effective and appropriate legislative response to the problem of computer crime is a hybrid approach involving the amendment of existing provisions as well as the addition of new provisions carefully drafted to address only those aspects of computer crime which truly are unique.

I. LEGISLATIVE DRAFTING PROBLEMS

It is now a truism to say that the computer is crucial to the functioning of our entire economy, and that this economic dependence affects every other area of society. One computer expert flatly states that "there is no person or organization that is not affected by the use of this invention." He concludes: "There is no turning back. Society could not revert to the days of manual processing of information even if it wanted to do so."

Two recent developments in this "computer revolution"—the proliferation of the personal computer, and the merging of computer and telecommunications technology—are of particular importance to the legal community. Small, relatively inexpensive computers have made personal computer use practical and affordable; central data-processing departments of large


12. Id. at 355.

13. See Smart, Rolling the Dice in the U.S. Portable Computer Crap Shoot, ELECTRONIC BUS., Oct. 1983, at 66 (portable computers are perhaps the fastest growing segment of personal computer market). See also A View From the Top, COMPUTER DECISIONS, Sept. 15, 1983 at 16, 24 (interviews with R. Martini, pres. of Bergen Brunswick Corp., and J. Dembeck, Corporate V.P. and Treas. of Olin Corp. discussing the "new breed" of executives who depend upon their personal computers) [hereinafter cited, respectively, as Martini Interview, Dembeck Interview]. Ticer, Gunfight at High Noon: TI versus the Competition, ELECTRONIC BUS., Oct. 1983, at 58 (the U.S. personal computer market estimated at $6 billion in 1983, up from $100 million in 1981).


15. Miller, Computing On The Go, INFOSYSTEMS, Oct. 1983, at 52 (users' descriptions of
business and government institutions no longer have a monopoly on this tool. Use of the personal computer is increasingly necessary to the work of individual employees and is being purchased in record numbers by private users as well.\textsuperscript{16}

Advances in telecommunications have brought long-range computer power within the reach of these individual users by giving them the ability to "talk" to other computers at great distances.\textsuperscript{17} This combination of computer and telecommunications technologies has resulted in an entirely new mega-industry,\textsuperscript{18} responsible for a completely different approach to the storage, retrieval and transmission of information.\textsuperscript{19} However, like every other major influence on society, this development is not without its concomitant problems:\textsuperscript{20}

For better or worse, the union of these two dynamic technologies appears destined to work profound social and economic changes, with ramifications extending far beyond their respective industries. Getting rid of the old regime is just a start. Already politicians and scholars fuss and fret about the implications, for good and ill, of post-industrial America's metamorphosis into the "information society." Further in the future, its realization deferred more for political than technological reasons, looms the "global village," a whole world wired together by intelligent, high-speed communications channels.\textsuperscript{21}

---

personal experiences with portable computers), 62 (predictions of price declines); Miller, \textit{Voice Systems, Picking up Momentum}, INFOSYSTEMS, Nov. 1983, at 84 (description of Voicemail system using computers and telephone lines).

16. \textit{See generally supra note 13.}

17. Consumers are now looking for ways to communicate with one another using their new-found home-computer power. \textit{See Van Gelder, Modems: Close Encounters of the Computer Kind}, Ms., Sept. 1983, at 61 (writer's experiences with "talking to strangers" through electronic mail and bulletin board system). Business, of course, is also seeking to take advantage of telecommunications networks through computers. \textit{See Dembeck Interview, supra note 13, at 27.}


21. Hillhouse, \textit{supra note 18}, at 95. \textit{See also Lautsch, supra note 10}, at 115 (public policy makers need to address potential problems); \textit{Information Is Power, COMPUTER DECISIONS, Sept. 15, 1983, at 10 ("techniques unimaginable last year threaten to transform in-
This rapidly expanding area of technology has caught the law as well as the layman by surprise. Because of these two relatively recent developments, behaviors associated with computer abuse by employees as well as private individuals are becoming more common, creating, at the very least, serious losses for business and government, and serious jurisdictional problems for prosecutors and judges.

Legislators attempting to create laws which justly and fairly address the issues brought to the forefront by new and perhaps unfamiliar technology face several difficult problems, some of which are inherent in any legislative drafting task. For example, each lawmaker will bring his or her own perceptions of computers and computer crime to bear on the problem, as well as varying individual levels of expertise.22

Growing dependence upon the computer has created a serious economic, social and political problem: dealing with crimes involving computers and their data. The problem has developed at a rate which can only be likened to that of advances in computer technology itself. It is also a problem as limitless as the technology which spawned it.

For an analysis of the growth of the computer industry in developing countries, and a description of the constraints which these countries impose on foreign involvement with that growth, see The Computer Industry, supra note 18, at 36-38, 55.

22. This rapid development and accelerated rate of change may be more than the layman can easily assimilate, and may lead to feelings of awe or fear, tinged with resentment, toward computers, a common reaction to any experience which cannot be easily incorporated into previous experiential boundaries. Considering the different effects of computers on our individual "legal consciousness," one writer muses:

On a physical level, the computer is staggering in its ability to . . . manipulate enormous quantities of information [concerning] money, complex mathematical equations, physical goods, or repetitive tasks. All fit within the computer's grasp.

On an intellectual level, . . . systems and information science theories have caused everyone to . . . think in new ways. For instance, . . . the law has no consistent answer to the demand to redefine "property" in view of the value of information in the computer environment.

[The] third kind of reaction . . . [is] a response on a mythical level. [It] does not affect the way we think, but shapes the stories we tell ourselves when we do not know what to think. . . . [U]narticulated feelings about computers affect the whole realm of computer crime.

A. Defining Computer Crime

In any emerging field of law, definitional problems are particularly troublesome to legislators. Computer-related crime poses special concerns in this area. In the first place, commentators cannot agree on a single philosophical approach as to what constitutes computer crime, and, therefore, as to the point at which an action relating to a computer becomes a criminal action. Within the subproblem of defining employee-related computer abuse, for example, there are four levels of improper use of an employee's computer which concern institutions. The crucial issue is: at what point should these activities be termed "criminal conduct?"

The first level of employee-related computer abuse is commonly referred to as "simple, unauthorized use" of the computer, and might take the form of the employee playing games, printing out calendars or personal correspondence, keeping small amounts of personal information in his or her files, or breaking the organization's computer security codes to view protected data "for the fun of it." At this level, neither monetary gain to the employee

23. An especially vexing definitional problem is that, even within the computer industry, there is no general agreement on the basic definition of "computer."

Within the [computer] field, four powerful trends—dramatic improvements in computer capabilities, rapid evolution of their physical characteristics, steady expansion of their application and usage, and constant enhancement of their embodied price/performance ratios—have all necessitated constant modification of the standard labels used in computer product classification. Even then, the terminology always trails the marketplace.


"Experts" writing in the field range from attorneys (Susan Nycum) to technologists (John Taber) to researchers (Donn Parker). See Bureau of Justice Statistics, U.S. Dept. of Justice, Computer Crime: Electronic Fund Transfer Systems and Computer Crime 39, Exhibit 4-1 (1982) (comparing definitions of computer crime by Carroll, Parker, Schabeck and others) [hereinafter cited as Bureau of Justice Statistics]; Note, Addressing Computer Crime Legislation: Progress and Regress, 4 Computer/L.J. 195, 196-97 (1983) (comparing definitions of Parker, Taber, Ingraham, and Nycum). Parker's definition of computer abuse is the broadest: "Any intentional act associated in any way with computers where a victim suffered, or could have suffered, a loss, and a perpetrator made, or could have made, a gain." Parker, Computer Abuse Research Update, 2 Computer/L.J. 329, 333 (1980). See also Kling, Computer Abuse and Computer Crime as Organizational Activities, 2 Computer/L.J. 403, 407 (1980) ("computer abuse" is a better term than "computer crime" or "computer fraud," since it allows "a larger variety of problematic practices to be addressed").

24. Sokolik, supra note 10, at 368. For a discussion of the possibility that the provisions in pending federal legislation may be interpreted as criminalizing such activities, see infra notes 138-42, and accompanying text. See also People v. Weg, 113 Misc. 2d 1017, 450 N.Y.S.2d 957 (1982) (N.Y.C. Crim. Ct.) (employee alleged to have used his employer's computer to trace racehorse bloodlines and to prepare and print his resume). For a more
nor intent to harm the employer is involved; this would seem to be relatively innocuous behavior of the sort that most programmers vehemently defend. However, some experts have offered the opinion that this form of computer abuse is "prevalent," and "can cause, in the aggregate, serious disruption of the employer's computer operations." In addition, whether carried on by employees or by outside computer users who gain access to the system without authorization, these so-called "harmless" activities may later develop into deliberate misuse of the system. The next level of computer abuse is unauthorized use of the employer's computer for personal gain unrelated to the main function of the computer, a form of "moonlighting" using the employer's computer facilities. In one case, programmers used their employer's computer for their own computerized sheet-music arranging company. More serious yet is the third level of abuse, where an employee manipulates the computer, using a fraudulent scheme in a clearly criminal act, in such a way as to give him or her gain to the detriment of the employer, the public, or the employer's customers. Finally, an employee can use computer skills to intentionally sabotage the employer's operations or erase crucial data. Various attempts at definition have considered all these activities as

complete discussion of the underlying facts of this case, see N.Y.L.J., Jan. 11, 1983, at 2, col. 3.


27. Sokolik, opus note 10, at 368.

28. United States v. Kelly, 507 F. Supp. 495 (E.D. Pa. 1981). The programmers were charged with theft of computer services, but they were convicted of mail fraud because they failed to state in their advertising brochures that they were using their employer's computer. In one case, a $5000-per-week bookmaking operation at a Ford Motor plant was exposed. Employees had used the company's word processor to store information and to print out betting tickets. Data Gathered on Computers' Role as Accomplices, L.A. Daily J., Apr. 8, 1983, at 14, col. 3 [hereinafter cited as Data Gathered].

29. See, e.g., People v. Calandra, 117 Misc. 2d 972, 459 N.Y.S.2d 549 (Sup. Ct. 1983) (vice president of New York bank's commercial loan department charged with grand larceny for allegedly diverting funds to co-defendants in guise of loans transferred by computer to "borrower's" checking accounts). The Los Angeles District Attorney's office reported the case of an employee who tapped into his employer's computer to alter his income tax records to show a larger withholding. See Prosecutors Try to Curb Growing Computer Crime, L.A. Daily J., Aug. 25, 1983, at 1, col. 6 [hereinafter cited as GROWING COMPUTER CRIME]. The employee intended to claim a larger refund. Id. at 16, col. 2.

well as others to be within the category of "computer crime."\textsuperscript{31}

One commonly held view is that "the computer has changed both the form and the means by which the traditional crimes . . . of fraud, theft, larcency, embezzlement, sabotage, extortion and conspiracy are perpetrated . . . ."\textsuperscript{32} Although some writers classify these behaviors as "a new array of criminal conduct,"\textsuperscript{33} such activities do not constitute a completely different category of criminal behavior at all. To consider illegal computer-related behavior other than as ordinary crime which uses a computer either as a tool (as in thefts of money or information), a subject (as in computer date-matching frauds), or an outright object of attack (as in physical destruction of computer disks or terminals)\textsuperscript{34} is to assume erroneously that just because computer technology is new, any behavior related to it must also be new.\textsuperscript{35} Consequently, lawmakers should examine carefully the related assumption that completely new legislation must be drafted in order to deal effectively with these problems. As developed below, they can use any one or a combination of three basic approaches to criminalizing computer-related conduct: an asset/loss approach,\textsuperscript{36} a behavioral approach,\textsuperscript{37} and a victim/perpetrator approach.\textsuperscript{38}

\textsuperscript{31} Raysman & Brown, supra note 26, at 1, col. 1 (behavior which has been termed "computer abuse" ranges from using the employer's computer to play games to deliberately causing patient's death by altering medical files).

\textsuperscript{32} Sokolik, supra note 10, at 362, 364.

\textsuperscript{33} Id. As one government study noted:

Many computer-related crimes can be prosecuted successfully without delving deeply into the technology. Many more of them, however, are sufficiently different from traditional crimes relative to the occupations of perpetrators, environments, modi operandi, forms of assets lost, time scales, and geography to identify the subject as a unique type of crime that warrants explicit capabilities and action.

\textsuperscript{34} D. Parker, Crime by Computer 17-18 (1976).


\textsuperscript{36} This approach asks: What did the victim have and what did he or she lose? D. Parker, Fighting Computer Crime 244 (1983) (focusing on asset/loss aspect of computer crime is more useful and usable concept than focusing on "technical" means of causing loss, as it avoids having to identify rapidly changing technology that could make statutes obsolete).

\textsuperscript{37} This approach asks: How was the crime committed? See Note supra note 23, at 196-97 (discussing Susan Nycum's adoption of this approach).

\textsuperscript{38} See Kling, supra note 23, at 411.
Each approach emphasizes a different aspect of the criminal behavior involved. The asset/loss approach defines computer abuse by focusing on the harm incurred—that is, on the assets involved and the valuation of their loss. Under this approach, appropriate categories might be financial crime (taking money via computer), informational crime (taking valuable data via computer), theft of property (taking computer merchandise for sale or personal use), theft of services (unauthorized use of a computer system), and vandalism (intentional damage or destruction of a computer or computer material). Legislation based on this approach could very likely use and modify existing statutes, since a well defined legal structure already exists to punish offenses against property. The major modification necessary would be the inclusion of computer-type assets in the statutory definitions of property.

Others who have studied the problem of the definition of computer crime prefer to focus on the methods used by computer abusers. The question becomes, then, not how much did the victim lose, but how was the abuse perpetrated? Under this approach, the categorization of various intrusive behaviors depends upon an understanding and analysis of the physical make-up of the computer system. For example, abuses can be grouped according to "the manner of misappropriation," focusing on the fact that one can obtain information from a computer system through "five key points": (1) the data entered into the computer; (2) the programs used to run it; (3) the electronic components of the central processing unit; (4) the printed or coded output, and (5) the remote transmission of information over telephone lines or microwaves. At each point, a determination of how the abuse is committed is critical. Since the criminal behavior is defined in relation to the new technology, it is perceived as an entirely new type of behavior which would require the proscription of entirely

40. Id.
41. A number of state statutes have adopted this approach: See infra note 142.
42. See, e.g., Note, supra note 23, at 197, 198 (describing the approach of Nycum).
43. Id. at 197.
44. Id.
45. Note, supra note 23, at 198 (describing contention of Sokolik). But see BUREAU OF JUSTICE STATISTICS, supra note 23, at 17 (distinguishing consumer, corporate, and internal crime, thus placing emphasis on where abuse is committed).
new legislative provisions.\textsuperscript{46}

A third approach is to focus on the \textit{identities} of perpetrators and victims.\textsuperscript{47} This scheme differentiates between computer crimes committed by individuals and those committed by businesses, the latter being an area which most analysts have ignored.\textsuperscript{48} Categories of computer crime in this approach are nearly congruent with categories of white-collar crime:

1. Crimes by persons operating on an individual, \textit{ad hoc} basis, for personal gain in a non-business context (. . . personal crimes). 2. Crimes in the course of their occupation by those operating inside businesses, Government, or other establishments, or in a professional capacity, in violation of their duty of loyalty and fidelity to employer or client (. . . abuses of trust). 3. Crimes incidental to and in furtherance of business operations, but not the central purpose of such business operations (. . . business crimes). 4. White-collar crime as a business, or as the central activity of business (. . . con games).\textsuperscript{49}

Several states have recognized these distinctions by including a separate scheme of penalties for violations by organizations as opposed to violations by individuals.\textsuperscript{50}

In summary, although computer related crime is not necessarily a new type of criminal behavior, it does not fit easily within existing legislative definitions. In deciding which of the many attributes of computer crime to emphasize in a definitional or classification scheme, legislators must become attuned to such definitional differences, since the determination of what constitutes a crime must necessarily affect the legislation drafted to proscribe it.

The present language of many existing state penal laws is simply too narrow to encompass computer technology and the concepts which accompany it.\textsuperscript{51} Technology has outpaced legislation,

\textsuperscript{46} See, e.g., N.Y.S. 8977, 207th Sess. §§ 146.05-.10 (computer trespass), 146.20-.25 (computer tampering) (1984).
\textsuperscript{47} See, e.g., Kling, supra note 23, at 412.
\textsuperscript{48} Id. at 411.
\textsuperscript{50} ALASKA STAT. § 11.46.985 (1978); ARIZ. REV. STAT. ANN. § 13-2316 (1978 & Supp. 1984-1985); COLO. REV. STAT. § 18-5.5-102 (Supp. 1984); UTAH CODE ANN. § 76-6-703 (Supp. 1984).
\textsuperscript{51} Marbach, supra note 1, at 46 (quoting Harvard law professor Miller as decrying...
and the language of these statutes either does not apply at all or must be stretched to cover computer-abuse situations. Prosecutors complain that they are forced to "shoehorn" computer offenses into laws which were drafted long before computers were invented.\textsuperscript{62}

The inadequacy of existing legislative provisions is evidenced not only by their failure to provide a sufficiently comprehensive definitional scheme but also by the fact that the mechanisms they employ for valuing losses may well be inappropriate in the context of computer crime. Obviously, these problems are interrelated. Assume, for example, that legislators could agree on a simple definition of computer program: "The list of instructions that tells a computer to perform a given task or tasks."\textsuperscript{63} If a person destroys or sabotages a "program" in a computer, what, exactly, is lost? Is the program a product, or is it a service? Is it a tangible object or a set of intangible electronic impulses? If it is intangible, can it still be "property?"\textsuperscript{64} Suppose further that a caller electronically transfers intangible information (either a computer program or other data stored in a computer) from a computer in one location to another. Even if that information is printed out at the intruder's end of the transaction, it also remains in the original computer. Were the language of existing larceny statutes to control, would it be reasonable to conclude that such information had been "taken" or that its owner had been "permanently deprived" of its use?\textsuperscript{65}

\textsuperscript{62} Computer Security, supra, note 1, at 130. See, e.g., United States v. Kelly, 507 F. Supp. 495 (E.D. Pa. 1981) (defendants who used employer's computer for personal sheet-music arranging business convicted on mail fraud charges instead of for theft of computer services). \textit{See also} Note, supra note 23, at 201 (discussion of shortcomings of traditional criminal laws when applied to computer crimes); Lautsch, \textit{supra} note 10, at 106 (difficulty of conceptualizing "software" and "firmware").


\textsuperscript{64} See \textit{id. Ward}, brought under California Penal Code § 499c(b) (West 1970), held that electronic impulses transmitted over telephone line were not tangible articles within the meaning of the statute. \textit{See also} United States v. Seidlitz, 589 F.2d 152 (4th Cir.), \textit{cert. denied}, 441 U.S. 922 (1978) (defendant convicted of wire fraud only because he used telephone across state lines; the case illustrates the difficulty of applying traditional concepts of "property" and "taking" to electronic impulses). \textit{But see}, e.g., Hancock v. Texas, 402 S.W.2d 906 (Tex. Crim. App. 1966), \textit{aff'd sub nom.} Hancock v. Decker, 379 F.2d 522 (5th Cir. 1967) (computer software is property, even if intangible).

"The interpretation of whether acts of theft or damage to computer programs are crimes varies widely from state to state. The answer often hinges on whether a computer
The problem is complicated further by the fact that, in many states, information is not given the statutory protection accorded to tangible property.\textsuperscript{56}

Clearly, better definitional and valuation guidelines are needed to assess the damage from computer crime.\textsuperscript{57} Since computer information may not be protected under existing statutes, valuation of the harm done to the victim might have to be assessed in terms of computer time used, which is measured only in milliseconds, rather than in terms of the value of the information. In any situation concerning the theft of a computer program or of information stored in a computer,

it would clearly frustrate the rightful owner's reasonable and understandable expectation [of justice] to be told that he had suffered no wrong that the court would hear until the form of unlawful possession became one which could be folded into a glider. For the very practical purpose provided by the program [i.e., running the computer], reduction to print on paper would be wholly irrelevant.\textsuperscript{58}

One possible way to view and value the loss to an owner of a computer program which is misappropriated through electronic stealth is to note that he or she no longer enjoys exclusive or as much control over dissemination of the information contained therein.\textsuperscript{59} However, if the concept of computer-stored information were incorporated into a state's larceny statute under the definition of property, and the definition of "appropriation" covered

program is considered property under a state's statutes or case law." Volgyes, 2 COMPUTER/L. J. 385, at 399 (1980). See Note, supra note 23, at 199 (notion exists in law of theft that in order to be termed "stolen," property must be tangible and must physically change possession).

New York's larceny statute defines property as "money, personal property, thing in action, evidence of debt or contract, or any article, substance or thing of value, including any gas, steam, water or electricity, which is provided for a charge or compensation." N.Y. PENAL \textsc{Law} \textsection 155.00(1) (McKinney 1975). Provisions (3) ("Deprive") and (4) ("Appropri- ate") both state that criminal behavior occurs if the major portion of the property's economic value is lost to the owner.

56. \textsc{Law Enforcement Assistance Admin.}, U.S. Dep't of Justice, The Investigation of White Collar Crime: A Manual For Law Enforcement Agencies 2 (1977) [hereinafter cited as \textsc{White Collar Crime}].

57. See Note, supra note 23, at 200. Depending on the definition, a program could be worth the $12 cost of the disk it is written on or the $25,000 worth of business it means to a company. See also Volgyes, supra note 55, at 399 (even in states which have passed computer abuse laws, if the "actual monetary value of the lost program is not clear, its theft may be only a misdemeanor").

58. Ingraham, supra note 35, at 433.

59. \textsc{Criminal Justice Resource Manual}, supra note 33, at 141-42.
situations in which computer programs and data were copied but not printed out, no convoluted interpretations of the taking and the resultant loss would be necessary.  

Without clear statutory provisions which encompass intangible electronic impulses, the law continues to be ambiguous. "The price of [this] uncertainty in [the language of the] criminal law is not paid by the prosecutor, but by the victim and the community whose interests are thereby excluded from consideration by the courts." This ambiguity can and should be corrected with definitions designed to cover new technological areas. However, in drafting new legislation, care must be taken to include only those

60. Recognition of a property right in intangible information stored in a computer would follow a general trend in other areas of the law. Fourth amendment search and seizure law, for example, shows a movement away from a general judicial hesitance to recognize a privacy interest in the (intangible) spoken word. Though courts once were reluctant to curtail electronic surveillance activities as unconstitutional invasions of privacy, recent decisions have recognized that the "search" of a person's words by means of electronic surveillance without his or her permission is as much an invasion of privacy as a warrantless search of tangible papers or possessions. See generally A. Miller, THE ASSAULT ON PRIVACY (1971); Galloway, The Uninvited Ear: The Fourth Amendment Ban on Electronic General Searches, 22 SANTA CLARA L. REV. 993 (1982) (long-range electronic surveillance is a general search, despite fact that person is not touched physically; such surveillance must therefore be subject to the requirements and restrictions of the fourth amendment); Carter, Book Review, 93 YALE L.J. 581 (1984) (reviewing I. Pool, TECHNOLOGIES OF FREEDOM (1983)); Gillers, Book Review, 92 YALE L.J. 731 (1983) (reviewing R. Berger, DEATH PENALTIES: THE SUPREME COURT'S OBSTACLE COURSE (1982)); McNulty, Dalia v. United States, The Validity of Covert Entry, 65 IOWA L. REV. 931, 933-39 (1980) (tracing development of fourth amendment law as it applies to interception of communications).

Further developments in technology warrant further refinements of the concept of "search and seizure" and the language used to describe violations in this area. The present federal wiretap statute forbids unauthorized monitoring of conversations except for law enforcement officers who have obtained a warrant. 18 U.S.C. §§ 2511, 2516 (1982); 18 U.S.C.A. §§ 2511, 2516 (West 1970 & Supp. 1984). However, conversations are now possible via computer; when an individual types a message into his or her computer, the message is converted into electronic impulses which can be sent to another computer via telephone wires. But the federal statute defines prohibited interception of another's communications as "the aural interception of information," id., a definition into which electronic bits and bytes simply cannot fit. Civil liberties groups are concerned that this discrepancy creates a dangerous opportunity for governmental abuse of individual privacy. Loophole in Law Allows Interception of Computer Data, L.A. Daily J., Dec. 27, 1983, at 12, col. 3. Local, state, or federal law enforcement officers might conduct computerized electronic surveillance without the court approval required for conventional wiretaps. By monitoring telephone calls and electronic mail, authorities can gather information about an individual's dealings with others which could be used to establish relationships among members of organized groups. Id.

61. Ingraham, supra note 35, at 436.
definitions which are necessary, and to avoid technical jargon. Once the definitions are clear, valuation of such intangible assets should be easier.

B. Other Legislative Drafting Considerations

1. Prosecutorial discretion. Effective computer-crime legislation could greatly mitigate the dangers of prosecutorial discretion. The leeway law enforcement officials are afforded under present statutes is illustrated by the comments of one federal prosecutor who declared that his office would be reluctant to prosecute teenagers who enter a computer system with no intent to deprive because “[i]t would be excessive to prosecute this matter as a five-year felony.” Although a computer criminal may cause damage to computer files worth hundreds of thousands of dollars, he or she, if prosecuted at all, may well receive an extremely light sentence simply by virtue of being a teenager or white-collar worker. Moreover, light sentences are sometimes handed down when the prosecution finds it too difficult even to establish the value of the harm done to the victim. This often occurs when information rather than money is taken, or when information in computer files is destroyed or altered. A consistent prosecutorial policy must be evolved in these cases, but clear statutory provisions are a necessary first step toward achieving such a policy.

62. Id. at 437.
63. Marbach, supra note 1, at 47 (quoting Rudolph Guiliani) (Marbach mistakenly calls him “Richard”).
64. The value of any particular computer file, of course, depends on the method of valuation. See supra note 57.
65. See generally White Collar Crime, supra note 56, at 1, 2, 8-10 (discussion of public’s and prosecutors’ perceptions of “real” crime and white-collar crime and reasons why prosecutors are reluctant to accept cases of white-collar crime). See also Sokolik, supra note 10, at 572 (discussion of discrepancy in sentencing); Becker, supra note 22, at 454 (examples of light sentences). But see Nagel & Hagen, The Sentencing of White Collar Criminals in Federal Courts: A Socio-Legal Exploration of Disparity, 80 Mich. L. Rev. 1427 (1983) (no empirical support for contention of sentencing disparity).
67. See Roddy, The Federal Computer Systems Protection Act, 7 J. Computers, Tech. & L. 343, 364 & n.150 (recommends sentencing guidelines rather than a rigid statutory standard so that “the courts can tailor penalties commensurate with the seriousness of the crime”). See also infra notes 57-62, and accompanying text (dealing with valuation of computer-related material).
2. Inexperience of prosecutors, judges, juries. Many prosecutors, judges, and juries are handicapped by inexperience with computer technology, and those in states which already have computer crime bills are further handicapped by lack of experience dealing with and interpreting these laws. Limited computer literacy may make some prosecutors reluctant even to accept a case involving computer crime, particularly if the victim's losses are small.

As a practical example of the difficulties authorities face in a case of this type, a prosecutor who wishes to search a computer file for a particular piece of information must (1) have the necessary technical knowledge to do so, and (2) draft a search warrant such that the judge will also understand what the prosecutor is looking for and how it can be recognized. Some agencies have instituted educational programs to introduce prosecutors to computer technology and the techniques of successfully prosecuting a case of computer abuse, but the effects of non-computer-literate prosecutors, judges, and juries will probably be felt for at least another generation. In the meantime, the most non-technically

69. Sokolik, supra note 10, at 360; Raysman & Brown, supra note 25, at 1, col. 1.
70. Becker, supra note 22, at 443. One prosecutor's personal statement concerning this issue was that:

I was wholly unprepared on the fatal morning when my boss told me to write a search warrant for the recovery of a computer program that a citizen was complaining had been stolen. The following hours convinced me that I had much to learn, and but for luck we may well have had to leave unredressed a theft that was later valued at $0.5 million.

72. D. Parker, supra note 36, at 239. Ingraham comments: "If so esteemed a leader of the legal profession as retired Associate Justice Arthur J. Goldberg can flaunt his ignorance of computer technology, it should not be thought that the courts will soon be as familiar with computers as they have become with horseless carriages." Ingraham, supra note 35, at 438 (footnote omitted, citing Beeler, Ex-Justice Goldberg Sees Privacy Major Issue, Computerworld, Apr. 9, 1979, at 20, col. 1). One guidebook advises prosecutors to “[m]ake the whole case as basic, simple and free from computer technology and terminology as possible. . . . [J]uries do not have to understand telephony to convict an obscene telephone caller.” Criminal Justice Resource Manual, supra note 33, at 125. It advises them to use
oriented legislation possible should be used in computer abuse cases. It follows that making judicious use of familiar legislative language and provisions would be most effective.

3. **Uncertain jurisdiction.** Uncertain jurisdiction presents serious obstacles for both federal and state authorities. Although federal prosecutors may be somewhat better equipped to deal with computer crime than their counterparts at the state level, they do not always have jurisdiction to enter the investigation, and often must proceed under a related statute such as one addressed to tax evasion or wire fraud.\(^7^8\) The question of jurisdiction can be equally perplexing for state authorities, when, for example, a court must determine whether it has jurisdiction over an out-of-state telephone caller who accesses a local computer without authorization.\(^7^4\)

4. **Attitudinal obstacles.** The white-collar employee who uses a computer to defraud or to steal data from a public or corporate institution very often has no previous police record, and, like the computer hacker, rationalizes that so impersonal an activity could hardly be considered a crime against other persons.\(^7^5\)

In addition to the rationalizations of outside computer abusers and employees, two other attitudinal factors create problems for business and law enforcement. First is the "heroizing" which

---

73. For a list of some of the 40 or more federal criminal statutes which may be used to prosecute computer crimes and abuse, see Volgyes, *supra* note 55, at 396-97.

74. A federal computer crime statute "would remove the requirement that telephones or other forms of illicit computer penetration take place across a state line in order to justify federal prosecution." Sokolik, *supra* note 10, at 379.

75. For a discussion of some ethical issues faced by computer users, see D. Parker, *supra* note 36, at 137 (ethics questionnaire answered by students and businessmen), 191-226 (chapters on ethical and moral situations). Parker claims that even though more individuals use computers in the course of their work, "opportunity is not the basis of most computer-related crimes. The acts are usually committed by amateur white-collar criminals who are trying to solve deep personal problems." Parker, Book Review, *Computer Decisions*, Oct., 1983, at 234 (reviewing A. Norman, *Computer Insecurity* (1983)) (emphasis added) These individuals may consider their actions to be "borrowing" rather than stealing, and the impetus may be financial stress brought on by alcoholism or drug abuse. Alternatively, the motive may be revenge for some real or fancied injustice encountered on the job. See Miles, *supra* note 30, at 210. However, there do not seem to be any statistically relevant studies upon which to base a definitive conclusion.
often occurs when the press reports the story of a computer crime. The facts are often presented with a tongue-in-cheek tone, even by legal journals, and the public is subtly encouraged to admire the cleverness and derring-do of the criminal rather than to condemn the crime. The impersonal nature of the “victim” (a machine, a large firm, a bank) surely has much to do with this public attitude. However, this heroizing is ill-advised, since even non-malicious access to a forbidden data base could have tragic consequences. Business and government are beginning to realize the potential damage that unauthorized computer use can wreak, and are attempting to deal with the problem using both technical and legal weapons.

Another problem is that large businesses, universities and financial institutions tend not to report incidents of computer abuse, fraud, or theft. If the abuse is committed by an employee, a company, in order to protect its reputation of competence, in-

76. See, e.g., Microkid Raids: The FBI Cracks Down, Time, Oct. 24, 1983, at 59 (thousands of teenagers use home computers and telephones to break into larger systems around the country); Data Gathered, supra note 28, at 14, col. 3 (“legendary” teenager reported to have shut down the telephone directory assistance board in Pasadena, broke into a computerized lineage of thoroughbred horses, destroyed half a data bank, breaking the code of U.S. Leasing International’s computer, and altered or destroyed data worth $250,000).

77. See, e.g., Ohleand & Berreby, In Flux: A Grave Development on the Computer Front, Nat’l L.J., Apr. 26, 1982, at 47, col. 1 (accounts payable clerk created false company in name of child who died at the approximate time her boyfriend was born, made several payments to account, then erased computer record, quit job, and went on spree with stolen money).

78. There were conflicting reports concerning the Milwaukee students’ break-in of the Sloan-Kettering computer system described, supra note 1. One report indicated that one day’s billings for a physician were wiped out. See Drinkard, supra note 1, at A-8. Another report, however, was more ominous; it stated that the medical records of some cancer patients under radiation treatments were altered. Laws in U.S. Called Inadequate to Block Abuse of Computers, N.Y. Times, Sept. 18, 1983, at 42, col. 1 [hereinafter cited as Laws Called Inadequate].

79. Computer Security, supra note 1, at 127 (dialback systems request password from the caller, disconnect, then automatically dial back number of user with that password; encryption systems encode data before transmission; use of identification codes). See also Gillard & Smith, Computer Crime: A Growing Threat, BYTE, Oct. 1983, at 398, 414 (description of the newest security techniques—voice and fingerprint recognition).

80. See infra notes 100-46 (federal and state legislative response), 147-205 (New York State legislative response) and accompanying text.

81. Raysman & Brown, supra note 26, at 2, col. 2; Computer Security, supra note 1, at 130.
tegrity, and inviolability, may choose to handle the problem with employment sanctions rather than risk public exposure of the culprit, since to disclose the wrongdoing might reveal internal procedures or weaknesses in the system. This dearth of reported computer crimes makes it much more difficult for law enforcement and legislatures to gather information which might help them gain experience with this type of crime for the purposes of future prevention and prosecution.

Finally, computer technologists argue that unused computer time which would be completely wasted otherwise should be available to anyone who has the skill to take advantage of it. "This perquisite . . . is a part of the short tradition of computing," and to criminalize such behavior, technologists believe, would, in itself, be a crime, because it would stifle the creative instinct of programmers and technological people who learn by "playing around with" computers.

5. Civil versus criminal penalties. One of the thorniest problems legislators must solve is choosing which approach to take in relation to "the most ubiquitous computer related abuse—that of unauthorized, though legal, use of computer services." For example, employees who have authority to use a computer in the course of their work may also use it during lunch hours or after work for personal purposes which are not per se criminal. One argument for imposing civil rather than criminal penalties for this type of abuse is that business ought to bear some of the burden for policing the use of its own computers. Furthermore, "[r]emedial civil liability is more appropriate than criminal sanctions because it will require the abuser to compensate the true vic-

82. Sokolik, supra note 10, at 359.
83. ISSUE BRIEF, supra note 71, at 2.
84. Donn B. Parker, computer security expert, was named project director of Stanford Research Institute's study for the U.S. Dep't of Justice. The new study will detail prosecutions in 18 states which have computer fraud laws. Data Gathered, supra note 28, at 14, col. 3.
85. D. PARKER, supra note 36, at 138-39. For an explanation of computer timesharing and "idle" time, see Roddy, supra note 68, at 355 n.95 (rebuttering Taber's argument by pointing out that free computer time was classified as property in U.S. v. Sampson, 6 Computer L. Serv. Rep. (Callaghan) 879 (N.D. Cal. 1978)).
86. See generally Taber, supra note 25.
tim of the misappropriation. Thus, compensation serves to make the injured party whole while simultaneously deterring the abuser from committing the wrongful behavior again.88

In drafting appropriate provisions, lawmakers must decide where to draw the line between civil and criminal liability. Perhaps intent to defraud might be the benchmark. With regard to damages or punishments allowable, they must also consider whether to create penalties in relation to the amount of personal gain to the perpetrator or the amount of loss to the victim.89

Because of a lack of previous experience in dealing with computer crime90 and a dearth of reliable statistics upon which to base informed opinions,91 legislators, computer crime experts, and computer technologists find themselves differing sharply on the best legislative approach to the problem. They disagree on whether to enact completely new legislation or to amend existing laws, and whether to support federal or state legislation, or both.92

Many authorities favor enactment of new legislation specifically directed at computer abuse and advance a number of reasons to show why such new legislation is necessary.93 They assert, for example, that computer users are uniquely vulnerable as victims because of the sensitivity of data or potentially greater amounts of money involved. Passage of new legislation designed to punish computer criminals would alert the public, the government, and computer manufacturers to the pressing need for increased security.94

Further, new laws are needed to give notice that computer

88. Id. at 401-02.
90. See supra notes 68-72 and accompanying text.
91. BUREAU OF JUSTICE STATISTICS, supra note 23, at iii, 61 (quoting John Taber).
92. Raysman & Brown, supra note 26, at 2, col. 4.
93. Laws Called Inadequate, supra note 78, at 1, col. 1; Ingraham, supra note 35, at 429-30; Comment, supra note 23, at 195.
94. Raysman & Brown, supra note 26, at 2, col. 2. See, e.g., Ognibene, The Law Must Recognize That Computers Pose National Security Risks, L.A. Daily J., July 21, 1983, at 4, col. 3 ("almost everything of value to a corporation is in computers: financial transactions, research, marketing plans, personnel records"); executives of large Japanese computer concern who admitted buying confidential IBM documents could have obtained information through computers without leaving "an incriminating trail of evidence"); BUREAU OF JUSTICE STATISTICS, supra note 23, at ix, 34 (potential of corporate EFT (Electronic Funds Transfer) crime is high because of large dollar volume of transactions processed each day).
abuse is increasing, and that the applicability of current legislation is uncertain. Finally, adequate legislation will make evidence gathering and prosecution easier, reducing the necessity for prosecutors to rely on related statutes when bringing charges against computer abusers.

While not conceding that there is such a phenomenon as computer crime, at least one commentator argues that new legislation is completely unnecessary, since, "the real legal problems of computer crime are . . . the results of . . . bungled indictments, improper prosecution, and in general, a lack of understanding of the law. . . . [I]n every known case in which a real crime occurred, the prosecutor has been able to secure a conviction under one or more existing laws." 

95. Sokolik, supra note 10, at 374. Parker emphasizes other reasons why computer crime deserves our attention: "[T]he occupations of the perpetrators, the methods of the crime, its environment, the forms of assets involved, timing (milliseconds and less), and geography (long-distance computer communication) can differ markedly [from traditional crime situations] when computers are involved, and thus warrant special treatment." Parker, supra note 23, at 334; D. Parker, supra note 36, at 244.

96. Sokolik, supra note 10, at 375. Another commentator asserts that [a] person potentially subject to a criminal law . . . is entitled to a non-elastic reading of law to properly forewarn him that the conduct is sanctioned. . . . Furthermore, extension of the scope of a law by the courts to bring certain activities not foreseen by the draftsmen within its scope may encroach on the legislative function, a boundary judges strive not to cross.

Roddy, supra note 67, at 352, n.74. In this connection, Judge Juiler stated in People v. Weg, 113 Misc. 2d 1017, 1023, 450 N.Y.S.2d 957, 961 (1982), that New York may "find a need to regulate, even by penal sanction" conduct such as Weg's, but the judge refused to encroach on the legislature's function. See N.Y.L.J., Jan. 11, 1983, at 2, col. 3.

97. Sokolik, supra note 10, at 374, 375. Concerning the last two points, it is "absurd," according to one federal prosecutor who is in favor of new legislation, to "[require] that the victim prepare evidence of an injury other than that with which he is really concerned . . . . " Ingraham, supra note 35, at 430. "The so-called computer crime bills have recognized and sought to redress this problem." Id. He continues:

To the extent that the law prohibits theft, it is difficult to see the social benefit of compelling the prosecutor to characterize the forbidden activities in a less than accurate guise in order to pass the law's threshold. Burglary and rape, for example, need not be prorated in a rental mode to obtain the law's protection, because the interest that each law protects is recognized as deserving protection. Information, regarded by government, industry, and academia as a significant item of value, deserves no less protection.

Id. at 434.

98. Taber, supra note 87, at 527, 528 (emphasis added, citation omitted). Taber's definition of "real crime" does not include the kinds of activities described supra note 24 and accompanying text. See also D. Parker, supra note 36, at 240 (most prosecutors able to bring charges under existing laws).
Legislative action is necessary for a variety of reasons, some of which are similar to problems inherent in all white-collar crime and some of which are unique to computer crime. If additional legislation will reduce ambiguities in the law, then it behooves legislators to act accordingly. But addressing the problem with completely new legislation could be superfluous, confusing, and may lead to inequities. On the other hand, a judicious combination of new provisions and appropriately amended legislation would certainly be a more effective means of reducing those ambiguities. As developed in the following sections of this Comment, a hybrid approach would be the most sensible and effective legislative course, at least in New York. Some provisions, such as existing fraud and embezzlement statutes, can be effectively applied to the computer criminal who uses a computer as a tool to defraud banks or other businesses. However, these laws are inadequate to deal with those who access computers without authorization to obtain or destroy information.

II. Federal and State Legislative Response

Because of the problem of prosecutorial discretion discussed above, one argument against enactment of federal computer crime legislation is that it would be more harmful than helpful to small business victims. If the losses of these victims were relatively small, overburdened prosecutors might not have enough staff or funding to pursue their causes, with the unfortunate result that they could be left without an effective remedy.

One Congressional response to this dilemma has been the passage of the "Small Business Computer Crime Act." Recognizing that "[a]fter a computer crime is committed, the small businessman may not be able to rely on the criminal justice system for help," and that "[l]aw enforcement officials encourage the preventive approach which costs far less than . . . a successfully prosecuted case," the Act amends the Small Business Act to create a task force to study the effects of computer crime on small busi-

99. Laws Called Inadequate, supra note 78, at 1, col. 1.
100. See supra notes 63-67 and accompanying text.
103. Id.
A resource center responsible for the dissemination of information regarding computer crime will be established to help evaluate available security systems. The House Committee on Small Business concluded that this Act would be "an inexpensive, common sense response to the growing problem of computer crime against small business" and that it would enable small concerns to better evaluate the security of their computer systems so that the losses due to crimes committed by computer can be minimized.

The main thrust of this legislation, then, is as a cost-cutting, preventive, informational measure. These are admirable purposes, but do not effectively address the problem of prosecutorial discretion. Although the Act might prove to be a valuable adjunct to effective state legislation, passage of such state legislation also should be encouraged in order to deal adequately with the impact of computer crime on small businesses. Given the geographic breadth and jurisdictional complexity of computer crime, additional federal legislation is needed as well.

Because of the multistate and interstate nature of computer operations, and especially because of developing computer networks, uniform state legislation on computer-related crime would be most effective. Since achieving uniformity in state laws is unlikely, however, federal law may be essential, especially in cases where the interpretation depends on facts, concepts, and evidence that are themselves so dependent on technology. (citation omitted)

If it is conceded that federal legislation is desirable, what kind of federal legislation would be effective? As yet, Congress has not agreed on an answer. No federal computer crime law has been passed, although several bills have been introduced, and each has suffered the twin criticisms of being both too general and too specific.

The first federal legislation was introduced in 1977 and

104. Computer Security and Education Act, supra note 101, § 3.
105. Id. § 4.
106. H.R. REP. No. 423, supra note 102, at 6.
107. See generally THE COMPUTER INDUSTRY, supra note 18, at 21 (discussion of worldwide expansion of computer use). One implication of the tremendous growth rate of computer use is that perhaps some modifications will have to be made to international law to accommodate technological advances.
108. Volgyes, supra note 55, at 400.
submitted to the Senate Judiciary Committee. The following year, the bill’s sponsor, Senator Abraham Ribicoff, introduced S. 240, a slightly modified computer-crimes act, but like the first bill, it, too, was never reported out of committee. Some discussion of the weaknesses of this proposed legislation is warranted, since these bills seem to be the starting point of many legislators’ thinking on the subject of how to draft a computer crime bill.

The Ribicoff bills would have criminalized two types of computer-related behavior. The first is “computer fraud”: using a computer to plan or execute a fraud or to fraudulently obtain “money, property or services . . . .” The bill also would have criminalized intentional, unauthorized access to a computer, or the alteration, damage or destruction of a computer, computer software or data. Conviction of either offense would result in a substantial fine, up to fifteen-years imprisonment, or both.

S. 240 was immediately criticized by some computer experts sympathetic to the technologists’ point of view as being much too broad in scope, since the “intentional and unauthorized access” language would have criminalized much “incidental personal use [that] is without pecuniary motive.” Moreover, the provision criminalizing the use of a computer to devise a scheme to defraud would have made a criminal of anyone who created such a scheme but never actually put it into practice.

In addition, the bill’s definition of “computer” came under attack from two sides. The bill defined a computer as “an electronic device which performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic im-
Unfortunately, this definition is broad enough to include such devices as pocket calculators, memory typewriters, and some digital watches, thus making the unauthorized use of these devices a crime. At the same time, others complained that the too-specific language of the definition limited coverage to current technology, and thus advances in that technology would immediately result in outmoded provisions.

In 1983, Representative Bill Nelson, who drafted Florida's computer-crimes act as a state legislator, introduced H.R. 1092, which is based in part on S. 240. This proposed federal legislation attempts to improve on the shortcomings of the previous bills, but does so with limited success. Like the Ribicoff bills, the new bill's coverage is broad; it would protect all federal computer systems, those of federally insured financial institutions, and those which engage in interstate commerce or use interstate facilities. The basic framework of H.R. 1092 is also similar to that of the Ribicoff bills in that its intent is to prohibit the use of a computer for fraud or theft and to criminalize the damage or destruction of computer-stored information.

The new bill goes further, however. In an apparent effort to protect authorized users of computer programs and systems against deliberate interference from intruders such as hackers or

117. Taber, supra note 25, at 532.
118. Sokolik, supra note 10, at 380 (quoting Nycum's criticisms of the federal bill). See also D. Parker, supra note 36, at 241-42 (extensive discussion of language used in definition of "computer").
120. 98th Cong., 1st Sess. (1983). The current Congress has five bills pending from its 1983 session which deal in some way with computer-related crime. Of these, H.R. 1092 and H.R. 4301 deal directly with computer fraud and abuse and impose rather substantial penalties for these activities. H.R. 4301 states:

Whoever willfully uses a computer capable of being programed and reprogramed in the course of normal operations, in a manner not authorized by the owner, shall, if such affects interstate or foreign commerce, in addition to any other punishment provided for the course of conduct which provided the elements of the offense under this section, be fined up to $100,000 or imprisoned not more than ten years or both. [Courts] shall not suspend the sentence in the case of a conviction of a person under this section or give that person a probationary sentence, nor shall the term of imprisonment imposed under this section run concurrently with any term of imprisonment imposed for an offense based on such course of conduct.
121. H.R. 1092, 98th Cong., 1st Sess. § 1028(a)(1), (2).
122. Id. § 1028(b).
disgruntled employees, one provision would criminalize intentional and unauthorized "denial of the use of a computer, a computer program, or stored information" to any rightful user. An example of this type of abuse might occur if a fired employee sabotaged a computer program before leaving "by planting a 'logic bomb' in the program, set to trigger at a specific date, shutting down the computer and preventing it from restarting."

Unfortunately, the words, "intentional denial of the use of a computer to any rightful user" can be interpreted to cover widely varying contexts. Similar language has been incorporated into proposed New York legislation. A critic of the New York bill offers a construction of that phrase which is equally plausible, especially to those without a technical background: language penalizing the intentional, unauthorized denial of computer services could conceivably make a criminal act out of a "mere, albeit deliberate, breach of contract to provide such computer services." Or, in yet another reading of the phrase, "if the [drafters'] intent . . . was to add criminal penalties to a situation where some form of political demonstration deliberately disrupted the operations of a computer facility, . . . existing statutes must suffice, or else the

123. See supra notes 1-9, 30, and accompanying text.
124. H.R. 1092, 98th Cong., 1st Sess. § 1028(b) (1983). The full text of this provision reads:
   Whoever intentionally and without authorization damages a computer described in subsection (a) or intentionally and without authorization causes or attempts to cause the withholding or denial of the use of a computer, a computer program or stored information shall be fined not more than $50,000 or imprisoned not more than five years or both.

Cf. the language of § 1028(b) in the Ribicoff bill, which deals with this issue:
   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 fifteen years or both.

legislature should draft unambiguous legislation with this specific object in mind."\textsuperscript{129} Since the language of this part of the provision lends itself so readily to these different constructions, it should be modified to reflect more clearly the drafters' intentions.

The basic definition of computer in H.R. 1092\textsuperscript{130} is an improvement over the one used in S. 240 because it differentiates between computers used in a business situation and those used for personal purposes. Also, although at present most computers are based on electronic technology, the new bill's definition takes note of possible changes and advances in this area and is careful to include any business computing device regardless of the technology used in its construction.\textsuperscript{131} In an attempt to meet the criticisms of overbreadth leveled against past definitions of "computer," H.R. 1092 specifically excludes those computers "designed and manufactured for, and . . . used exclusively for routine, personal, family, or household purposes," provided that they are not linked in some way to another computer.\textsuperscript{132} As examples of excluded devices, the bill mentions "automated typewriter" or "portable hand-held calculator."\textsuperscript{133} But the specificity of the exclusions is a two-edged sword: in a few years, this language could prove to be a severe limitation as technology once again exceeds available legislative labels.\textsuperscript{134}

\textsuperscript{129} Id.

\textsuperscript{130} H.R. 1092, 98th Cong., 1st Sess. § 1028(c)(1) (1983).

\textsuperscript{131} "[E]lectronic, magnetic, optical, hydraulic, organic or other high speed data processing device . . . ." Id.

\textsuperscript{132} Id.

\textsuperscript{133} Id. Parker responds: "Don't exclude devices; only exclude uses if necessary. Leave it to the courts to decide what is a computer and a significant violation within the technology of the times." D. PARKER, supra note 36, at 242.

\textsuperscript{134} Id. For example, the newest portable computers now weigh less than ten pounds and run on batteries. Too broad a definition of "computer" would include digital watches and calculators. Too narrow a definition would exclude technological changes. An example of a broad definition is "an internally programmed, automatic device that performs data processing." Florida Computer Crimes Act, Fla. Stat. Ann. § 815.03(2) (West Supp. 1984). A more narrow definition is Colorado's: "an electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network." Colo. Rev. Stat. § 18-5.5-101(2) (Supp. 1982).

Current technology already includes voice control of computers, see Gillard & Smith, supra note 79, at 416, and computers that "see," INFOSYSTEMS, Nov. 1983, at 14. See also News & Comment: Hello, Computer, COMPUTER DECISIONS, Oct. 1983, at 39 (voice recognition device recognizes up to 25,000 words, replaces microcomputer keyboard, with implications
In addition, objections to criminalizing the activities of technologists who use their employers' systems to "play" have not been entirely met. Although the bill includes a provision which requires a willful intent to damage the system or otherwise to prevent authorized users from using the computer services,\(^3\) it also makes it a crime to "use . . . a computer . . . [t]o knowingly convert . . . the property of another."\(^4\) The definition of property includes computer services,\(^5\) and computer services include "computer data processing and storage functions."\(^6\) Conceivably, then, an employee using his or her employer's computer to store personal information could come under the ambit of this provision. However, in some instances, it probably should. Some prosecutorial discretion in the area of unauthorized use by employees might be advantageous, and appropriate civil penalties could be used to provide for this situation.\(^7\)

Thus, although federal legislation is, on the whole, desirable given the inadequacy of present federal and state statutes in dealing with computer crime,\(^8\) and while this bill is an improvement in some respects over the Ribicoff bills, "[t]he unnecessary jargon and overemphasis on the drafter's 'computer literacy' has produced a bill which . . . is unclear as to purpose and meaning."\(^9\) Some further refinements and clarifications are necessary before the bill, if enacted, will have the desired effectiveness as federal legislation.

At least twenty state legislatures\(^10\) have responded to the

---

for the handicapped as well as for business); Optical Memory Could Make Today's Storage Obsolete, SMALL SYSTEMS WORLD, Oct. 1983, at 20 (8000 pages of typewritten text on card the size of a plastic credit card; advent of optical memory systems compared to Gutenberg's invention of movable type); Kashner, Business Trends: We Have Seen the Future and It Is AI [Artificial Intelligence], ELECTRONIC BUSINESS, Nov. 1983, at 36 (description of "computer based products that imitate human thought patterns").

136. Id. § 1028(a) (1983).
137. Id. § 1028(c)(3) (1983).
138. Id. § 1028(c)(4) (1983).
139. See supra notes 88-89 and accompanying text.
140. See infra notes 142-46 and accompanying text.
141. See Klasson Letter, supra note 127 (discussing H.R. 1092). Mr. Klasson's opinion of the definition of "computer medium" in § 1028(c)(7) of the bill is that it "verges on the metaphysical."
problem of computer abuse. However, the confusion about how to conceptualize computer crime, what actions to criminalize and what sanctions to put on those actions is evidenced by the fact that the types of behavior covered and the penalties imposed in each statute vary from mere violations, even for fraudulent activities, depending on the value of the improper use involved, to felonies, even for simple, unauthorized use by an employee. These collected state statutes have been called "a terrible patchwork," and some reports indicate that the effectiveness of state legislation has been limited. For example,

[a]bsent the determination of the value of stolen or damaged software, or . . . evidence of the computer abuser's fraudulent intent, criminal prosecutions under many state computer crime statutes are cumbersome . . . . Some prosecutors and judges who have specific computer crime statutes at their disposal, are reluctant to apply them to computer abuses because the statutes are simply variations on larceny or damage to property statutes. . . . [D]epending 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.

III. ACTION BY THE NEW YORK STATE LEGISLATURE

New York State also has experienced the uncertainty and problems associated with a lack of appropriate computer crime legislation. Recently, in People v. Weg, a computer programmer working for the New York City Board of Education was charged with theft of services for using the Board's computer for his own

---

143. See Comment, supra note 24, at 203-04. See, e.g., Fla. Stat. Ann. § 815.06(1), (2)a (offenses against computer uses; felony calling for term of imprisonment of up to five years and a fine of up to $5000).

144. D. PARKER, supra note 36, at 242.

145. Comment, supra note 24, at 203.

146. Id.

147. 113 Misc. 2d 1017, 450 N.Y.S.2d 957.
COMPUTER-CRIME LEGISLATION

The issue was whether the computer in the school board office, a public institution, constituted "business, industrial or commercial equipment" under New York State's theft of services provision. The statute requires that the services in question be "business" services, and that they be used to create a "commercial or other substantial" benefit for the alleged thief. In Weg, the charges were dismissed because the computer belonged to a governmental agency and, therefore, could not be considered "business, industrial, or commercial equipment." Moreover, Weg did not realize any pecuniary benefit from his activities. Weg claimed that these activities were commonplace and that he was being prosecuted in order to make an example of him. Legislators, attempting to avoid such unfortunate situations in the future, have introduced four computer crime bills, all of which are now pending before the New York State legislature.

The first, S. 3080, is modeled after one of the original federal bills, S. 240, and the Florida statute, that is, it is a "stand alone" statute, and creates an entirely new article in the penal law to deal with crimes termed "computer fraud" and "computer damage or destruction." Like the Florida statute, it places computer programs and data into a category called "intellectual property." A New York State Bar Association Report succinctly points out some of the shortcomings of this bill:

The two defined crimes, "Computer fraud" and "Computer damage or destruction", do not necessarily cover in a rational manner the variety of types of conduct to be addressed. "Computer fraud" appears in part to

148. Id. at 1018, 450 N.Y.S.2d at 958.
149. Id. at 1019, 450 N.Y.S.2d at 958.
151. Weg, 113 Misc. 2d at 1019, 450 N.Y.S.2d at 958.
152. Id. at 1024, 450 N.Y.S.2d at 961. See also N.Y.L.J., Jan. 11, 1983, at 2, col. 3.
153. Raysman & Brown, supra note 26, at 2, col. 3.
156. Fla. STAT. ANN. §§ 815.01-.07 (West Supp. 1984).
158. Fla. STAT. ANN. § 815.03(1) (West Supp. 1984); N.Y.S. 3080, 206th Sess. at § 196.00(9) (1983). This categorization has been criticized as superfluous, since there is "no reason to single out computer data for identification as 'intellectual property' when other products of the human intellect are not so defined in [New York State's] Penal Law." LEGISLATION REP'T No. 125, supra note 128, at 9.
duplicate other Penal Law provisions (e.g., larceny, fraud), but may be useful in that it does define, through the inclusion of "information" in the definition of property, a crime related to the theft of computerized information. Arguably, this function could more easily be accomplished by modifying the definition of "property" in the "larceny" article, Penal Law § 155.00 (this was the approach used to address the problem of theft of cable television services...).159

The second proposed statute, S. 3890,160 in contrast, uses a very simple approach to the problem by merely proposing to amend the definitions of property in the criminal mischief161 and larceny162 sections of the penal law to make computer programs, software, systems and networks "property" for the purposes of these sections. Aside from some serious doubt which may exist about the wording of some of the definitions of computer terminology,163 this scheme has the advantage of simplicity and would actually be fairly comprehensive, including within the ambit of the modified provisions such computer-related abuses as theft or destruction of programs, data, money, and even services. Theft of services, in turn, could conceivably be interpreted to include unauthorized computer use.

The criminal mischief statute, as it now stands, penalizes only damage or destruction of tangible property.164 Adding computer software and data to the property definition of this section would expose a criminal who damages tangible or intangible computer-related property to gradations of punishment according to the criminal intent of the perpetrator165 and the amount of the damage sustained by the victim,166 all within a framework of existing, familiar legislative provisions. By explicitly including computer programs, systems and networks in the larceny statute, any taking of such property would be similarly covered.

162. Id. §§ 155.00-.45.
163. N.Y.S. 3890, 206th Sess. § 1 (1983). The definitions are taken word for word from the federal proposal, S. 240, and accordingly suffer from the same weaknesses. See supra notes 117-19 and accompanying text.
164. See N.Y. PENAL LAW § 145.00 practice commentary (McKinney 1975).
165. Id.
166. Id.
Critics of a bill such as this point out, however, that it would not single out unauthorized computer use by any special proscriptions in the penal law. One school of thought is that this behavior is potentially serious enough to warrant a separate prohibition. Including computer-related definitions of property under criminal mischief might not adequately cover this type of abuse, since offenses above a class A misdemeanor in that article require intent to cause damage on the part of the perpetrator. In many situations where employees or hackers, for example, break security codes to "play around" with a computer's files without authorization but do not intend to cause harm, the potential for damage can still be very serious. Should public policy mandate the use of severe penalties for unintentional damage to computer programs or data in order to discourage unauthorized use of a computer? Again, the definition of "computer crime" is significant. Privacy and property concepts are involved, and legislators must make some rather difficult choices as to what values to protect. Questions arise as to whether civil penalties are more appropriate, as to the extent of a business's responsibility to protect its own sensitive data, and as to whether computer files in government agencies should be especially protected by law.

The third proposed statute, S. 494, answers the above criticism. It contains one new provision dealing specifically with computer crime: a prohibition against unauthorized computer use. It does not, however, contain separate provisions for computer fraud or computer damage or destruction.

The definition of "computer" in S. 494 is one of the least

---

167. LEGISLATION REP'T No. 125, supra note 128, at 17.
168. See N.Y. PENAL LAW §§ 145.00-.30 (McKinney 1975 & Supp. 1983-1984). Section 145.05 (criminal mischief in the fourth degree) requires intentional damage of another's property or reckless damage in an amount exceeding $250.00. Id. § 145.05. The permissible penalties for this offense range from a prison sentence of one year to unconditional discharge.
169. LEGISLATION REP'T No. 125, supra note 128, at 18. See also Laws Called Inadequate, supra note 76, at 42, col. 1.
171. Id. §§ 186.00-.30.
172. Id. § 186.00(1). As used in this provision, "computer" means a device or group of devices which, pursuant to a computer program, can automatically perform arithmetic, logical, storage and retrieval operations with or on computer data and can communicate the results, and includes any connected or directly related device, equipment or facility which enables the computer to store, retrieve or communicate to or from a person, an-
technical of all the definitions thus far discussed. It incorporates broader concepts such as “computer system” and “computer network” and leaves ample room for future technological advances. However, in its simplicity, it allows for the inclusion of calculators, typewriters, and watches. This is not a serious drawback, since the bill also differentiates between uses of computers, and exempts personal uses from the proscriptions provided for abuses of business computers.

The bill’s stand-alone provision calls for gradations in punishment for unauthorized computer use, and also incorporates penalties for using a computer in the commission of another crime. This section would thus mandate a double penalty: a penalty for the crime committed with the use of the computer, and a penalty for using the computer as an instrumentality of the crime. The bill’s drafters reason that, while the double-penalty structure is undesirable in relation to use of the computer for fraudulent activities (since existing state statutes are adequate in that area), the penalties mandated for unauthorized computer use are not unduly harsh, and these provisions will serve as much-needed notice that such behavior can be dangerously destructive.

Instead of creating further provisions to deal with abuses such as computer fraud or computer damage or destruction, the remainder of S. 494 would modify existing statutes to include these abuses within the definitions of traditional crimes such as larceny, theft of services, and tampering with public records.

The fourth and newest bill is S. 8977, a “program bill” developed by the New York State Attorney General’s office. S. 8977 defines and proscribes two new categories of criminal behavior. The first is “computer trespass,” which prohibits breaking se-
curity codes in order to use a computer without authorization.\textsuperscript{179} This offense is classed as a misdemeanor.\textsuperscript{180} However, the charge escalates to a felony,\textsuperscript{181} and the requirement that a security code be broken is omitted if the unauthorized use is for the purpose of committing another felony. Again, this reflects the drafters’ opinion that this situation warrants a double penalty.

The same double-penalty scheme is used for a second new category of criminal behavior, “computer tampering,”\textsuperscript{182} defined as intentional and unauthorized destruction of computer data or programs. The felony charge applies under this provision if the perpetrator uses the computer without authorization to commit another felony, or if the perpetrator was previously convicted of computer abuse either under the larceny provisions or under the theft of computer services provision.\textsuperscript{183}

The remainder of the bill is devoted to proposed amendments of five sections of the penal law.\textsuperscript{184} For example, the new definitions of “property” and “deprive” of section 155.00, the larceny provision, would be amended to encompass computer-related material.\textsuperscript{185} The amendments are designed to define as “property” computer services and computer material \textit{in any form},

\begin{itemize}
\item \textsuperscript{179} Id. § 146.05. The bill’s drafters chose to make breaking a security code part of the language of this provision to eliminate the possibility that an employee with authorization to use a computer would come under the ambit of the provision, regardless of the nature of that use. They reasoned that employee misuse is a matter best regulated by the employer, since business has an obligation to protect its property. Telephone interview with James Cantwell, member of Sen. Stafford’s staff (June 1, 1984).
\item \textsuperscript{180} N.Y.S. 8977, 207th Sess. § 146.05 (1984). A Class A misdemeanor carries a maximum sentence of one year, N.Y. PENAL LAW § 70.15 (McKinney 1975), and a fine of up to $1000 or two times the amount of gain from the offense, \textit{id.} § 80.05, or up to $5000 if the offense is committed by a corporation, \textit{id.} § 80.10. See also NEW YORK SENTENCE CHARTS 1985 (West 1985), at 15, for alternative permissible dispositions.
\item \textsuperscript{181} N.Y.S. 8977, 207th Sess. § 146.10 (1984). A Class E felony carries a maximum sentence of four years, N.Y. PENAL LAW § 70.00 (McKinney 1975), and a fine of up to $5000 or two times the amount of gain from the offense, \textit{id.} § 80.00, or up to $10,000 or two times the amount of gain from the offense if the offense is committed by a corporation, \textit{id.} § 80.10. See also NEW YORK SENTENCE CHARTS 1985 (West 1985), at 12, for alternative permissible dispositions.
\item \textsuperscript{182} N.Y.S. 8977, 207th Sess. § 146.20-.25 (1984).
\item \textsuperscript{183} Id. § 146.25.
\item \textsuperscript{184} Other amended provisions include: § 165.07 (unlawful use of secret scientific material); § 165.15 (theft of services); § 170.00 (forgery, which defines computer data or programs as written instruments for purposes of crime of forgery); and § 175.00(2)-(3) (which now include computer data and programs within definitions of “business record” and “written instrument” for purpose of false written statements).
\item \textsuperscript{185} N.Y.S. 8977, 207th Sess. § 146.00(5) (1984).
\end{itemize}
whether as programs, printouts, or data which is stored internally in the computer's memory.\textsuperscript{186} In addition, the definition of "computer material" attempts to address one of the primary concerns expressed above, that the valuation of the program lies in its utility to the owner, not in any assessment of its tangible worth.\textsuperscript{187}

A drawback of the language of the bill, however, is that it does not solve the problem which arises when material is copied from one computer to another but not reduced to tangible form.\textsuperscript{188} Section 146.00(5) of the bill defines "computer material" as "property" and specifies that it

\begin{quote}
means any computer data or computer program which is not, and is not intended to be, available to anyone other than the person or persons rightfully in possession thereof or selected persons having access thereto with his or their consent, which accords or may accord such rightful possessors an advantage over competitors or other persons who do not have knowledge or the benefit thereof, and, in the case of reproduction or recording, which reproduction or recording is not for home or personal use or is intended for resale.\textsuperscript{189}
\end{quote}

The bill also enlarges the provision prohibiting the unlawful use of secret scientific material by adding computer material.\textsuperscript{190} The problem becomes evident on analysis of the language of Section 155.05 of New York State's Penal Law, which sanctions larceny and the unauthorized use of property. To be guilty of offense under the larceny statute, a person must be acting "with intent to deprive another of property or to appropriate the same to himself or a third person . . . ."\textsuperscript{191} "Deprive" and "appropriate" are defined as withholding or exercising control over property, "permanently, or . . . under such circumstances that the major portion of its economic value or benefit is lost to [the owner]."\textsuperscript{192}

Consequently, the new bill may not cover the situation where computer material is copied from one computer to another, but still remains in the original computer. Destruction of the material in the original computer in addition to the transfer would make a person liable under this statute, but it is far from clear that merely

\begin{footnotes}
\item[	extsuperscript{186}] Id.
\item[	extsuperscript{187}] Id.
\item[	extsuperscript{188}] See supra notes 55-62 and accompanying text.
\item[	extsuperscript{189}] N.Y.S. 8977, 207th Sess. § 146.00(5) (1984).
\item[	extsuperscript{190}] Id. § 165.07.
\item[	extsuperscript{191}] N.Y. Penal Law § 155.05(1) (McKinney 1975) (emphasis added).
\item[	extsuperscript{192}] Id. § 155.00(3), (4).
\end{footnotes}
copying alone would bring a violator under the ambit of this provision.

It is possible that the drafters chose to leave this area intentionally ambiguous, since copyright law\textsuperscript{193} might cover many of these situations. Nevertheless, little imagination is necessary to construct many situations where neither the civil sanctions of the copyright laws nor the criminal prohibitions of the larceny statute would be applicable, even with the addition of "computer materials" to the definition of property in the penal code.

A second major problem lies in the definition of "computer material," which closely parallels the language used in the definition of "secret scientific material."\textsuperscript{194} "Computer material" is only information which "accords . . . rightful possessors an advantage over competitors or other persons who do not have knowledge or the benefit thereof . . . ."\textsuperscript{195} While it is arguably appropriate in the context of secret scientific material, such language may inject the prerequisite of competitive advantage too strongly into the burden-of-proof requirement relating to computer material. This, in turn, may adversely affect the prosecution for theft of computer material from the computers of government agencies or not-for-profit corporations. The requirement of competitive advantage may very well be too narrow to include advantages other than business advantages obtained by the taking of the information.

The definition of "computer materials," read in conjunction with other larceny provisions, also requires proof that the material taken (if a reproduction or recording) is not intended for home or personal use or for resale.\textsuperscript{196} Many computer hackers "take" information in these forms "for the fun of it": the language of this provision could eliminate all prosecution in these cases. Furthermore, the prosecution bears the burden of proof, whereas, in proposed section 165.07 (unlawful use of secret scientific material or computer material), the person accused must prove that the material was "reproduced for home or personal use and was not intended for resale." Consequently, if a prosecutor charged an al-

\textsuperscript{193} See 17 U.S.C.A. § 101, 117 (definitions of "computer program") (limitations on exclusive rights: computer programs).

\textsuperscript{194} N.Y. PENAL LAW § 155.00(6) (McKinney 1975).

\textsuperscript{195} N.Y.S. 8977, 207th Sess. § 146.00(5) (1984).

\textsuperscript{196} Id.
leged thief with larceny for the taking of property under section 155.05, the prosecutor’s burden of proof would be more difficult than if the charge were brought under section 165.07.

The bill also defines computer data as “information . . . [or] . . . concepts . . . which are being prepared . . . in a formalized manner . . . .”\(^\text{197}\) This language fails to cover raw data which is sometimes entered into a computer and stored, to be processed at a later time.

The definition of the phrase “Uses a computer or computer service without authorization”\(^\text{198}\) presents yet a third problem of proof for the prosecutor. Use of a computer without permission of the owner is “without authorization” when the user has actual knowledge that he is acting without permission or has been given notice to that effect.\(^\text{199}\) If a computer or computer service owner is unaware that the computer is being used without authorization, and does not give notice to that effect, the prosecutor must then prove that the unauthorized user has actual knowledge that he or she was abusing his or her rights to use the computer.

The juxtaposition of language in the computer trespass provisions may also pose problems for a prosecutor. Proposed section 146.05 (computer trespass in the second degree) requires that the trespasser overcome a security code. However, this requirement is not included in the companion section 146.10 (computer trespass in the first degree), which merely requires that the unauthorized user knowingly use a computer to commit or attempt to commit a felony. Thus, if a trespass is committed but the trespasser did not break a security code, and proof that the computer was used to commit a felony fails, prosecution under 146.10 fails. The prosecutor could not fall back on 146.05, since the “security code” requirement prevents it from being a lesser included offense of 146.10.

Finally, since prosecution under 146.10 is expressly limited to prosecution for felonies defined in the larceny provisions,\(^\text{200}\) it excludes prosecution for federal felonies and for non-penal law felonies such as might be found in banking and securities law.

If these problems can be worked out, S. 8977 would seem to

---

197. Id. § 146.00(3).
199. Id.
200. Id. § 146.10 (“any felony defined in this chapter”).
be the best approach so far to computer crime legislation. Its definitions attempt to address the major concerns of valuation and of striking a balance between generality and specificity. Overall, the bill does not unnecessarily duplicate existing legislation. "Although . . . some additional provisions must be added to New York State law in order fully to cover computer related crime, . . . our Penal Law broadly covers the traditional categories of crime into which . . . many aspects of computer related crime can be placed."201 In addition, judges and prosecutors, more familiar with the language of the existing provisions, will find it easier conceptually to fit computer abuse into the larceny statute, for example, if the definition of property is expanded to encompass technical terms such as "computer program" and "data."202

Moreover, the scheme of gradations of punishment is already well worked out in the existing statutes; there should be no unfortunate cases of bringing harsh felony charges against programmers who use their employer's computer to play Dungeons and Dragons or to print out calendars. Finally, using the framework of existing statutes to combat the problem of computer crime has the advantage of flexibility. New terms can be added and/or definitions modified as new technology warrants without drastically changing the law to everyone's confusion.

CONCLUSION

Although the necessity for completely new legislation is widely advocated, New York, in its legal approach to these problems, should not focus specifically and exclusively on "computer" crime. State legislators have two options available. They can adopt new legislation based on federal S. 240,203 creating a so-called "stand alone statute" which treats computer crime as a completely separate offense, or they can amend existing statutes to take into account new situations created by new technology.

The legislators must first carefully determine what actions in relation to a computer ought to be called criminal and what sanctions should be authorized for each of those actions. This is an

201. LEGISLATION REP'T. No. 125, supra note 128, at 4.
202. N.Y. PENAL LAW § 155.00(6) (McKinney 1975) would be amended to include these terms within the definition of "secret scientific material."
203. See supra notes 110-19 and accompanying text.
extremely difficult problem in light of the newness of the technology involved. And, indeed, the second consideration with which legislators must concern themselves is the very newness and rapidity with which these technologies are developing.\textsuperscript{204} The laws passed today must be broad enough to encompass further advances in technology, yet narrow enough not to criminalize innocent behavior. This would seem to be best accomplished by a careful expansion of the coverage of existing legislation, rather than a broad-brush approach which could be both overreactive and counterproductive.

It has been said by those who argue for expanding existing statutes that there are no new crimes, only new ways of committing them. Theft is theft, they argue, and it is not necessary to create an entirely new statute to punish those who steal by using a computer. A computer, after all, is only a mechanical accomplice. Others argue that since there are special statutes for armed robbery, hit-and-run offenses, and assault with a deadly weapon, there also should be a separate statutory prohibition of computer crime. However, each of these earlier offenses developed out of a need to provide additional protection against added physical danger posed by a new technological development. Most of the present concern about computer crime, on the other hand, arises from the increased risk of monetary loss resulting from the new technology. Indeed, it should be noted that in the future there may be little other method of theft; we are on our way to becoming a "cashless, checkless society."\textsuperscript{205} While computers may also be used to commit crimes which are not purely monetary, such as extortion, sabotage, theft of services, or even murder, there is no reason why the use of present statutes, suitably expanded by the inclusion of computer terms should not prove adequate and fair.

Amalia M. Wagner

\textsuperscript{204} Compare, S. 240's definition of "computer" with the description of new technology involving optical transistors which would replace transistors and electromagnetic impulses in computers. The article also describes work currently in progress to develop organic transistors, a development made possible by recent breakthroughs in genetic engineering. Friedman, Searching for a Successor to the Transistor, INFOSYSTEMS, Jan. 1984, at 30.

\textsuperscript{205} Sokolik, supra note 10, at 357.