Fordham Urban Law Journal

Volume 12 | Number 1 Article 2

1984

Computer Abuse: The Emerging Crime and the Need for Legislation

Elizabeth A. Glynn

COMPUTER ABUSE: THE EMERGING CRIME AND THE NEED FOR LEGISLATION

I. Introduction

Society is presently in the midst of a computer revolution.[1] Computers have become irretrievably intertwined with the economic, social and political aspects of society.[2] They are currently used in a broad spectrum of activities[3] by banks,[4] financial institutions,[5] federal,[6] state and local governments,[7] educational institutions,[8] health

---

1. BUREAU OF JUSTICE STATISTICS, U.S. DEPT. OF JUSTICE, COMPUTER RELATED CRIME LEGISLATIVE RESOURCE MANUAL iii (1980) [hereinafter cited as LEGISLATIVE RESOURCE MANUAL].

2. *See generally* Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMPUTER L.J. 353, 357 (1980) [hereinafter cited as Sokolik]; Roddy, *The Federal Computer Systems Protection Act*, 7 RUTGERS J. COMPUTERS, TECHNOLOGY & L. 343, 349-50 (1979) [hereinafter cited as RODDY]. *See also* NEWS RELEASE, prepared by Rep. Bill Nelson (D. Fla.) (Feb. 7, 1983) [hereinafter cited as NEWS RELEASE] (more than two million computer operators, programmers, and technicians come in contact with computers daily).

3. *See* Tunick, *Computer Law: An Overview*, 13 LOY. L.A.L. REV. 315 (1980).

4. Computers electronically dispense money, post deposits, transfer funds to pay bills, and maintain accurate balances in bank accounts. *See* Volgyes, *The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review*, 2 COMPUTER L.J. 385 (1980) [hereinafter cited as VOLGYES].

5. *See, e.g.*, Lynch, *Fidelity Group Unit Speeds Banks' Entry into Discount Stock Brokerage Business*, Wall St. J., June 18, 1982, at 12, col. 1 (stock exchange is relying more on computer automation); Witcher, *New Exchange Plans Commodity Trading through Computers*, Wall St. J., Aug. 5, 1982, at 29, col. 1 (increased computer use in commodities market); Hertzberg, *Insurance Relying More on Automation*, Wall St. J., Nov. 9, 1982, at 37, col. 3 (insurance industry is relying more on computer technology).

6. The federal government relies on over 15,000 computers to maintain records, disburse funds, and analyze information. *See* NEWS RELEASE, *supra* note 2. For example, the Department of Defense disburses over $25 billion a year through more than 3,000 computers; the Department of Health and Human Services processes over $80 billion worth of checks per year utilizing a computer. *See Federal Computer Systems Protection Act: Hearings on S. 1766 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary*, 95th Cong., 2d Sess. 3 (1978) (opening statement of Senator Biden) [hereinafter cited as *Hearings*].

7. State and local governments utilize computers in a variety of functions such as storing records and data, planning, budgeting, and word processing. *See* VOLGYES, *supra* note 4, at 385-86.

8. American schools possess more than 100,000 computers for school use and student training. *See* NEWS RELEASE, *supra* note 2. *See generally* Kolata, *Students Discover Computer Threat*, SCIENCE, March 5, 1982, at 1216-17.

care facilities,[9] businesses,[10] and industry.[11] The recent proliferation in computer use has created an enormous volume of processed information. While society has benefited from the emergence of the computer,[12] the new technology also has engendered a new type of crime:[13] computer crime.[14]

Computer crime falls into four categories:[15] (1) theft of money, financial instruments, property, services, or valuable data;[16] (2) unau-

---

9. Computers are prevalent in health care administration and patient treatment in hospitals. *See generally* Waldolz, *Computer Diagnosis of Medical Cases Gets Mixed Reviews*, Wall St. J., Aug. 19, 1982, at 7, col. 2; Shaffer, *Technology*, Wall St. J., Apr. 9, 1982, at 21, col. 1.

10. It is estimated that businesses rely on more than 56,000 large general purpose computers, 213,000 smaller business computers, 570,000 minicomputers, and 2.4 million desktop computers, with over three million computer terminals in business offices. *See* NEWS RELEASE, *supra* note 2. *See generally* Fowler, *Executives in the Next Generation*, N.Y. Times, Oct. 3, 1979, § 4, at 15, col. 2 (computers will play increased role for company executives in coming years).

11. Computers are used in the manufacturing process to store records of inventory, to maintain records of ordering, and in shipping, billing, and collections for products. *See* Bigelow, *The Lawyer's Role in the Computer Age* [1972-1979 Transfer Binder] 1 COMPUTER L. SERV. § 1-1, at 1-4.

12. *See generally* A. BEQUAI, COMPUTER CRIME 9 (1977); D. PARKER, CRIME BY COMPUTER ix (1976). Some would characterize the relationship between society and the computer as one of dependence since the use of computers is continually increasing in the government and private sector. *See* Becker, COMPUTER CRIME AND SECURITY, CONG. RESEARCH SERV. 1 (1983) [hereinafter cited as COMPUTER CRIME AND SECURITY]. *See also* Pollack, *Computer Disaster: Business Seeks Antidote*, N.Y. Times, Aug. 24, 1983, at 1, col. 3.

13. *See* LAW ENFORCEMENT ASSISTANCE ADMINISTRATION, U.S. DEPT. OF JUSTICE, COMPUTER CRIME vi (1979) [hereinafter cited as COMPUTER CRIME].

14. "Computer crime" does not have a uniform definition. Therefore, for the purposes of this Note, it is defined as any knowing, fraudulent, illegal act that involves a computer or knowledge of computer technology where loss has occurred. *See* Parker, *Computer Abuse Research Update*, 2 COMPUTER L.J. 329, 330-31 (1980). *See also* COMPUTER CRIME, *supra* note 13, at v.

15. *See* 96th Cong., 1st Sess., 125 CONG. REC. 1190 (1979).

16. This aspect of computer crime is given the most publicity. *See, e.g.*, Gerth, *Embezzling Case at Wells Fargo: Keys are Computers and Volume*, N.Y. Times, Feb. 23, 1981, at 1, col. 3 (Wells Fargo National Bank lost more than $2.1 million in a computerized embezzlement scheme involving a former bank officer and several boxing promoters); Lindsey, *U.S. Agency Reportedly Set up Suspect in Computer Bank Fraud*, N.Y. Times, March 20, 1979, at 1, col. 4 (computer consultant and former college professor, Stanley Mark Rifkin, gained access to computer codes at the Security Pacific Bank and, posing as a branch manager, used the bank's computer to steal $10.2 million) (for an extensive discussion of the Rifkin Case *see* Becker, *Rifkin—A Documentary History*, 2 COMPUTER L.J. 471 (1980)); Jensen, *F.B.I. Said to Find Equity Forgeries*, N.Y. Times, Apr. 20, 1973, at 39, col. 6 (computer used by Equity Funding Insurance Company to write thousands of phony insurance policies and then to sell the policies to reinsurers, which generated over $27 million); Ball, *Computer Crime*, TECHNOLOGY REVIEW, Apr. 1982, at 22 (college student, utilizing his computer expertise, developed a scheme whereby he employed Pacific Bell's

thorized access to computer time;[17] (3) illegal use of computer programs;[18] and (4) unauthorized acquisition of stored data.[19] The incidence of crime in these four areas is increasing rapidly[20] and will continue to proliferate.[21] Many commentators state that the criminal

---

computer to steal $1 million worth of telephone equipment); Fosburgh, *Chief Teller is Accused of Theft of $1.5 Million at a Bank Here*, N.Y. Times, March 23, 1973, § 2, at 1, col. 2 (bank teller at Union Dime Savings Bank in New York embezzled more than $1.5 million through falsifying data utilizing an elaborate computer scheme). For further examples of this type of computer crime see T. WHITESIDE, COMPUTER CAPERS (1978).

17. This occurs when employees use their employer's computer for personal reasons, such as compiling mailing lists for fraternal and church organizations, drawing Snoopy calendars, calculating personal financial data, or playing games. *See* Dotto, The New Computer Criminal, ATLAS WORLD PRESS REVIEW, Aug. 1979, at 25-26. At first glance, such computer abuse seems petty, but in the aggregate it is no longer insignificant. *See* Ball, *Computer Crime*, TECHNOLOGY REVIEW, Apr. 1982, at 22. Recently, students have also been discovered using school computer time for wrongful activity. *See* Kihss, *Computer Caper in Dalton School is a Closed Book*, N.Y. Times, July 7, 1980, at 49, col. 2 (students at Dalton, a private school in New York City, used teaching computers to invade a Canadian data communications network and in the process destroyed the files of two of the network's corporate customers).

18. Theft of computer programs was the basis for charges in Hancock v. Texas, 402 S.W.2d 906 (Tex. Crim. App. 1966), *aff'd sub nom.*, Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967) (defendant was convicted for theft of fifty-nine computer programs from his employer). *See also* Kleiman, *Hospital in City Reports Computer Tampering*, N.Y. Times, Aug. 19, 1983, at 1, col. 2; Treaster, *Trial and Error by Intruders Led to Entry into Computers*, N.Y. Times, Aug. 23, 1983, at 1, col. 5 (young men, using a home computer, gained access to and reprogrammed computer containing records of patients at Memorial Sloan-Kettering Cancer Center in Manhattan).

19. This occurs where the computer is used to acquire or alter stored data for personal gain. *See, e.g.*, Fuerbringer, *U.S. Says Ex-Aide Stole its Computer Data*, N.Y. Times, Feb. 23, 1983, at 1, col. 2 (former Federal Reserve Board economist was charged with wire fraud for allegedly tapping into Federal Reserve computer to obtain secret data about nation's money supply while working for E.F. Hutton & Co.); McQuiston, *2 Accused of Stealing Time on a School's Computer*, N.Y. Times, Feb. 15, 1981, at 55, col. 1 (New York District Attorney's office charged two former directors of The New York Institute of Technology's Computer Department with illegally using school's computer in data storage scheme, which netted them over $40,000, and used more than $200,000 worth of time on college's computer to operate scheme).

20. *See* SOKOLIK, *supra* note 2, at 358; *see also The Spreading Danger of Computer Crime*, BUS. WEEK, Apr. 20, 1981, at 86 ("the spellbinding advance of the computer age is also creating . . . a vastly expanded potential for computer crime"). Furthermore, very few computer crime cases are reported in formal court opinions; most of the cases are reported only in the newspaper. *See* [1972-1979 Transfer Binder] 6 COMPUTER L. SERV. § 5-6 (R. Bigelow ed.).

21. Legal scholars on computer crime believe there are many more cases of computer abuse that have been detected than have been formally reported or prosecuted. The reluctance to report such crime can be attributed to fear that publicity will cause substantial embarrassment to banks, businesses, and financial institutions,

justice system needs guidance through specific computer crime legislation.[22] Some commentators, however, argue that the present criminal laws are sufficient to combat computer abuse.[23]

This note examines the rapid increase in computer crime and concludes that traditional federal and state criminal codes are ineffective in the prosecution of such crime.[24] It analyzes both the need for legislation at the federal level and the pending federal computer crime bill.[25] Existing and proposed state computer crime statutes are also examined.[26] Current criminal statutes in most states, as well as the federal statutes, are inadequate.[27] Amendment of existing computer crime statutes would be adequate to combat computer abuse in some states.[28] New laws are required, however, in the states without computer crime statutes, as well as on the federal level.[29]

---

which build reputations on their ability to rely on technological competence. *See generally* Raysman & Brown, *Evolving Statutes on Computer Crime*, N.Y.L.J., Jan. 11, 1983, at 2, col. 1; D. PARKER, CRIME BY COMPUTER 16 (1976); *Beware: Hackers at Play*, NEWSWEEK, Sept. 5, 1983, at 42, 46.

22. *See* LEGISLATIVE RESOURCE MANUAL, *supra* note 1, at iii (criminal justice practitioners agree that guidance is needed concerning approach to computer crime investigations and prosecutions); *Laws in U.S. Called Inadequate to Block Abuse of Computers*, N.Y. Times, Sept. 18, 1983, at 1, col. 1 (prosecution of computer criminals is hindered because of lack of precise legislation); Burnham, *Laws to Bar Computer Misuse Remain Scarce*, N.Y. Times, Sept. 8, 1982, at 1, col. 4. *See also* Raysman & Brown, *Evolving Statutes on Computer Crime*, N.Y.L.J., Jan. 11, 1983, at 2, col. 4 (prompt need for computer crime legislation).

23. *See* Taber, *On Computer Crime (Senate Bill S. 240)*, 1 COMPUTER L.J. 517, 525 (1979) (crimes committed with computer involvement are already adequately covered by existing laws) [hereinafter cited as Taber]; see also *infra* note 79 for discussion of view that computer crime is sufficiently covered by traditional criminal laws.

24. Prosecuting the computer criminal presents special problems because the prosecutor is forced to base his charge on traditional legal theories that did not anticipate the technical aspects of computerization. *See Hearings*, *supra* note 6, at 11 (statement of Senator Ribicoff).

25. See *infra* note 72 for a discussion of this bill; see *infra* notes 58-62 for an analysis of the need for federal legislation.

26. *See infra* text accompanying notes 111, 112.

27. Presently, there is no federal computer crime statute. *See infra* text accompanying note 32. Nineteen states have computer crime provisions in their penal laws, leaving thirty-one states with no computer crime statutes. See *infra* note 91 and accompanying text for a list of state computer crime statutes. Of the enacted state computer crime statutes, none has been embraced by commentators as an ideal "model approach" to computer crime.

28. The nineteen states with computer crime statutes could amend their penal codes to conform with a consensus computer crime approach.

29. *See supra* note 27.

II. The Federal Level

A. Existing Federal Laws

Computer technology has changed the form and means by which traditional crimes may be perpetrated.[30] Moreover, it has created a new type of criminal conduct which the present federal criminal code has been unable to adequately curb.[31] Since no federal statute specifically addresses the use of computers for criminal purposes,[32] a federal prosecutor must charge and seek conviction under one of the nearly forty potentially applicable federal statutes.[33] However, none of these

---

30. Prior to the advent of computers, theft or embezzlement from banks or financial institutions required a physical taking of tangible property. Today the same result may be accomplished by a simple telephone hook-up to the institution's computer. Similarly, computers have facilitated easy access to data and statistical information now stored in computers. *See, e.g., Beware: Hackers at Play*, NEWSWEEK, Sept. 5, 1983, at 42. The FBI recently uncovered a Milwaukee-based group of children, who call themselves the "414s", who gained unauthorized access to over sixty business and government computer systems purely for fun. *Id.* at 46. Although charges were dropped against all involved, it was noted that prosecution under present criminal statutes would have been difficult because the prosecutor would need to prove criminal intent on the part of these "joyriding" children. *Id.*

31. *See* COMPUTER CRIME, *supra* note 13, at 131. Although computer crime is the same in name as other familiar types of crime, including fraud, larceny, embezzlement, theft, vandalism, burglary, extortion, and conspiracy, it differs significantly in application from traditional crimes in that computer loss may involve an intangible that is difficult to value or classify as property, which may be required by existing criminal statutes. *Id.* at vi; *see also* Nycum, *The Criminal Law Aspects of Computer Abuse: Part II: Federal Criminal Code*, 5 RUTGERS J. COMPUTERS & L. 297 (1976) (extensive discussion of existing criminal statutes as they may be applied to computer abuse). *See generally Laws in U.S. Called Inadequate to Block Abuse of Computers*, N.Y. Times, Sept. 18, 1983, at 1, col. 1 (lack of local and federal laws specifically applicable to computer crime is primary reason why few perpetrators are ever prosecuted for computer abuse).

32. While presently there is no federal legislation specifically aimed at computer crime, a proposed bill would make some computer abuse a federal crime. *See infra* note 73 and accompanying text.

33. *See Hearings on S. 240; The Federal Computer Systems Protection Act of 1979 Before the Subcomm. on Criminal Justice of the Senate Judiciary Comm.*, 96th Cong., 2d Sess. 1, 15 (1980) (statement of J.D. McFarlane) (approximately forty federal statutes could be applicable to control computer crime); *see also* Nycum, *The Criminal Law Aspects of Computer Abuse: Part II: Federal Criminal Code*, 5 RUTGERS J. COMPUTERS & L. 297, 305-22 (1976) for a comprehensive list and discussion of federal statutes applicable to computer crime and a division of the federal statutes into seven broad categories: (1) theft and related crimes, (2) abuse of federal channels of communication, (3) national security offenses, (4) trespass and burglary, (5) deceptive practices, (6) malicious mischief and related offenses, and (7) miscellaneous other statutes. All forty potentially applicable statutes are embodied in Title 18 U.S.C. §§ 1-6005 (1976).

statutes was designed originally to control computer-related criminal activity.[34] When seeking a conviction, the prosecutor must analyze the computer-assisted offense and attempt to "shoe-horn" the case into the most applicable existing federal statute.[35] Such an approach has substantial procedural and substantive difficulties.[36]

Only a handful of the nearly forty potentially applicable federal statutes actually have been used to prosecute computer abuse.[37] The more frequently applied statutes are the federal wire fraud statute,[38] the federal mail fraud statute,[39] the transportation of stolen property

---

34. *See supra* note 24 and accompanying text for discussion of difficulties inherent in prosecuting computer criminals under traditional statutes.

35. *See* SOKOLIK, *supra* note 2, at 373; *see also Computer Crime*, 19 AM. CRIM. L. REV. 499, 508 (1981) (discusses difficulties prosecutors face in trying to match specific computer crimes with existing criminal laws).

36. *Id.* at 507-08. The absence of specific state or federal legislation defining computer crime hampers the prosecutors' ability to prosecute; the impediments that computerization pose hinge on the prosecutors' inability to draft accusatory pleadings which identify a statutory prohibition with the conduct in question. *See generally* Becker, *The Trial of a Computer Crime*, 2 COMPUTER L.J. 441, 445 (1980); Ingraham, *On Charging Computer Crime*, 2 COMPUTER L.J. 429, 430 (1980); *Laws in U.S. Called Inadequate to Block Abuse of Computers*, N.Y. Times, Sept. 18, 1983, at 1, col. 1.

37. Although there are forty provisions in the federal criminal code under which the prosecution of computer criminals is arguably possible, certain provisions have been utilized more frequently, with varying success. *See* VOLGYES, *supra* note 4, at 396-97 (lists the most adequate sections); *see also supra* note 33.

38. *See* 18 U.S.C. § 1343 (1976). The statute provides:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communications in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both.

39. *See* 18 U.S.C. § 1341 (1976). The statute provides:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined not more than $1,000 or imprisoned not more than five years, or both.

statute,[40] and the theft and related offenses statute.[41] Analysis of case law illustrates that each of these statutes is ineffective as a prosecutorial device for computer crimes.[42]

The federal wire fraud statute[43] requires execution of a scheme to defraud through the misuse of interstate communication devices.[44]

---

40. *See* 18 U.S.C. § 2314 (1976). The statute provides:

Whoever transports in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud; or

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transports or causes to be transported, or induces any person to travel in, or to be transported in interstate commerce in the execution or concealment of a scheme or artifice to defraud that person of money or property having a value of $5,000 or more; or

Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce any falsely made, forged, altered, or counterfeited securities or tax stamps, knowing the same to have been falsely made, forged, altered, or counterfeited; or

Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce any traveler's check bearing a forged counter-signature; or

Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce, any tool, implement, or thing used or fitted to be used in falsely making, forging, altering, or counterfeiting any security or tax stamps, or any part thereof—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

This section shall not apply to any falsely made, forged, altered, counterfeited or spurious representation of an obligation or other security of the United States, or of an obligation, bond, certificate, security, treasury note, bill, promise to pay or bank note issued by any foreign government or by a bank or corporation of any foreign country.

41. *See* 18 U.S.C. § 641 (1976). The statute provides:

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $100, he shall be fined not more than $1,000 or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

42. *See infra* notes 48, 52, 53, 57, 59 and accompanying text.

43. *See supra* note 38.

44. *See* United States v. Condolon, 600 F.2d 7 (4th Cir. 1979) (successful prosecution of wire fraud depends on misuse of interstate communication facilities to

This statute has been utilized to prosecute computer criminals by expanding the definition of "property" to include computer impulses moving across interstate wires.[45] Case law indicates that the nature of computers causes problems when the statute is applied to computer crime.[46] The court must broadly construe the statutory requisites[47] in order to encompass computer offenses.[48]

---

execute any scheme or artifice to defraud); United States v. Cowart, 595 F.2d 1023 (5th Cir. 1979) (Government, in obtaining wire fraud conviction, must prove use of interstate communications and criminal intent to defraud); United States v. Louderman, 576 F.2d 1383 (9th Cir.), *cert. denied*, 439 U.S. 896 (1978) (for successful prosecution, Government need not prove success of scheme nor that loss occurred; it need only prove there existed a scheme to defraud and use of interstate communications); United States v. Corey, 566 F.2d 429 (2d Cir. 1977) (Government need only show that defendant participated in a scheme to defraud and that interstate wires were used to further the scheme); United States v. O'Malley, 535 F.2d 589 (10th Cir.), *cert. denied*, 429 U.S. 960 (1976) (in a prosecution under this section, the Government need not prove success of scheme or that intended victim suffered loss; it need only prove use of interstate communications in furtherance of a scheme to defraud); United States v. Houlihan, 332 F.2d 8 (2d Cir.), *cert. denied*, 379 U.S. 828 (1964) (crime of fraud by wire complete where there is unlawful scheme and use of interstate or foreign telephonic, telegraphic, or electronic means of effectuating scheme).

45. *See White-Collar Crime: Computer Crime*, 18 AM. CRIM. L. REV. 370, 374-78 (1980).

46. See *infra* note 48 and accompanying text for extensive discussion of case law illustrating the difficulties.

47. *See supra* note 44 and accompanying text.

48. *See* United States v. Giovengo, 637 F.2d 941, 945 (3d Cir. 1980), *cert. denied sub nom.*, Paladino v. United States, 450 U.S. 1032 (1981), in which the defendants, two customer service agents for an airline at the Greater Pittsburgh Airport, devised a scheme whereby they defrauded their employer of cash paid by passengers for one-way airline tickets. *Id.* at 942. The Third Circuit, broadly interpreting the wire fraud statute, upheld the defendants' conviction, finding that the statute covered wire impulses generated by the airline's main computer in Kansas City, Missouri, which were then used to imprint tickets at the Pittsburgh airport. *Id.* at 944-45. In applying the wire fraud statute to this computer offense, the court relied heavily on the fact that these tickets were essential to the execution of the fraudulent scheme. *Id.* at 945. *See also* United States v. Alston, 609 F.2d 531 (D.C. Cir. 1979), *cert. denied*, 445 U.S. 918 (1980). There the defendant was found guilty of having executed a scheme to defraud whereby he was paid to have an accomplice falsify computerized credit records of individuals who had difficulty obtaining credit. *Id.* at 533. The altered credit records were then sent for approval to various lending institutions, ultimately allowing these individuals to obtain credit to purchase automobiles and other items. *Id.* Although the scheme involved computer tampering, the circuit court affirmed the district court's liberal construction of the wire fraud statute to encompass defendant's actions. *Id.* at 538. In United States v. Seidlitz, 589 F.2d 152 (4th Cir.), *cert. denied*, 441 U.S. 922 (1978), the defendant, who operated his own computer business in Virginia, gained unauthorized access to his former employer's computer located in Maryland. The defendant obtained the computer program via electronic signals over interstate telephone lines connected to his Virginia office. *Id.* at 154-55. The Fourth Circuit affirmed the conviction of defendant, finding suffi-

The federal mail fraud statute[49] also has been utilized with some success in cases involving computer crime.[50] Application of this statute requires fulfillment of two statutory requisites: (1) a scheme to defraud, and (2) a mailing for the purpose of executing the scheme.[51] The mail fraud statute requires a broad interpretation of what constitutes a mailing to enable the prosecution of computer crime.[52] Moreover, some courts have had difficulty applying this statute to computer criminals where the facts of a particular case failed to meet the statutory requisites.[53]

Under the transportation of stolen property statute, it is illegal to transport stolen goods, securities, property worth $5,000, or cash in that amount across state lines.[54] Prosecutors have faced procedural

---

cient evidence to deem that the transmission of electronic signals across state lines constitutes the transportation of "property" within the meaning of the federal wire fraud statute. *Id.* at 160. The prosecutor's success in *Seidlitz* rested on the fact that the defendant had telephoned the computer in Maryland from his home in Virginia. If the defendant had not transmitted the programs across state lines, the wire fraud statute would have been inapplicable.

49. *See supra* note 39.

50. *See Computer Crime*, 19 AM. CRIM. L. REV. 499, 501 (1981).

51. *See* United States v. White, 673 F.2d 299, 302 (10th Cir. 1982) (essential elements of mail fraud are (1) existence of scheme to defraud and (2) utilization of mails in furtherance of the scheme); United States v. Melton, 689 F.2d 679, 684 (7th Cir. 1982) (to prove violation of mail fraud statutes, victim need not actually be defrauded or suffer loss); United States v. Hasenstab, 575 F.2d 1035, 1039 (2d Cir.), *cert. denied*, 439 U.S. 827 (1978) (for successful prosecution under this statute, it is enough to prove that a scheme to defraud existed and that it was foreseeable that the scheme would utilize the mails); United States v. Baren, 305 F.2d 527, 528 (2d Cir. 1962) (the two necessary elements for violation of this section are (1) formation of a scheme with intent to defraud, and (2) use of mails in furtherance of that scheme).

52. *See* United States v. Kelly, 507 F. Supp. 495 (E.D. Pa. 1981), in which the defendants organized a computerized sheet music arranging and engraving company through the unauthorized use of their employer's computer. In addition, they used the mails to distribute brochures describing their business scheme. *Id.* at 497. Their fatal mistake, however, was in failing to state in the brochure that they were using their employer's computer to execute the business. The court, reading the mail fraud statute very broadly, convicted the defendants. *Id.* at 508-09. Had the defendants given credit to their employer, prosecution under the mail fraud statute would have been futile. Whether the defendants could have been successfully prosecuted for their computer abuse is at best an uncertainty. *See also* United States v. Curtis, 537 F.2d 1091 (10th Cir.), *cert. denied*, 429 U.S. 962 (1976) (defendant devised scheme involving computerized dating; court held there was substantial evidence in record to establish elements of mail fraud and conviction was upheld).

53. *See* United States v. Computer Sciences Corp., 511 F. Supp. 1125 (E.D. Va. 1981), *rev'd*, 689 F.2d 1181 (4th Cir. 1982), *cert. denied*, 103 S. Ct. 729 (1983) (Fourth Circuit determined that dismissal of wire fraud and mail fraud charges was error, reasoning that district court's application of statutes' scope was too narrow).

54. See *supra* note 40 for statute.

and substantive problems when applying this statute to computer offenses.[55] One court declared the statute inapposite since the computer misappropriation did not entail a physical transportation between two states.[56] Another court offered strained reasoning in order to bring the defendant within the purview of the statute.[57]

The theft and related offenses statute prohibits embezzlement, theft, unauthorized conversion, sale or disposition of federal property.[58] The ineffectiveness of current federal statutes in dealing with computer offenses is illustrated by application of this statute. Although courts have found the statute applicable to the theft of com-

---

55. See *infra* notes 56 & 57 for case law illustrating the difficulties. *See also White-Collar Crime: Computer Crime*, 18 AM. CRIM. L. REV. 370, 376 (1980) (application of transportation of stolen property statute to computer crime raises several problems).

56. In United States v. Seidlitz, *supra* note 48, the defendant was charged with intent to defraud through the use of interstate wires and with interstate transportation of stolen property. The trial court dismissed the latter charge and the Fourth Circuit affirmed. 589 F.2d at 155, n.12. The district court found that the programs Seidlitz misappropriated via electronic impulses over telephone lines were not really carried off because they were still within the computer. Seidlitz had merely reproduced them via a remote terminal. The logical inference from the court's decision is that, for successful prosecution of a computer crime under this statute, actual physical transportation of the original property across a state line is needed.

57. *See* United States v. Jones, 553 F.2d 351 (4th Cir.), *cert. denied*, 431 U.S. 968 (1977), in which defendant fraudulently obtained and cashed checks payable to herself. Defendant employed someone to alter accounts payable data entered into the computer of his employer, a Canadian subsidiary of Whirlpool Corp. As a result of this entered data, false accounts payable documents were set up in the defendant's name, and the computer printed checks with facsimile signatures payable to the defendant, which should have been payable to Whirlpool. Defendant was charged with the interstate transportation of fraudulently obtained checks. *Id.* at 352-54. The district court dismissed the indictment on the grounds that the checks were forgeries and therefore did not violate the statute under which defendant was charged. 414 F. Supp. 964, 967 (D. Md. 1976). The Fourth Circuit reversed, concluding that the issuance of the checks by computer constituted an act of fraud rather than forgery, and thus fell within the statute. 553 F.2d at 355-56. Accordingly, it has been recognized that if indeed the checks had been found to be forgeries and the indictment dismissed, there would probably have been no federal statute under which to charge the defendant. *See* Gemignani, *Computer Crime: The Law in '80*, 13 IND. L. REV., 681, 705 (1980) [hereinafter cited as *Gemignani*].

58. See *supra* note 41 for statute. *See generally* United States v. Evans, 572 F.2d 455 (5th Cir.), *reh'g denied*, 576 F.2d 931, *cert. denied*, 439 U.S. 870 (1978) (for successful prosecution under this statute, the Government must prove embezzling or stealing public money, property, or records, and that it resulted in some actual property loss); United States v. Trcinski, 553 F.2d 851 (3d Cir. 1976), *cert. denied*, 431 U.S. 919 (1977) (receipt of stolen goods requires actual carrying away); United States v. Fleetwood, 489 F. Supp. 129 (D. Or. 1980) (for prosecution for embezzlement of savings bonds under this section, Government must show presence of control sufficient to establish federal interest over property seized).

puter time, computer programs, and computer printouts,[59] successful prosecution of a computer crime utilizing this statute hinges on how liberally the court will interpret the statutory requisites.[60]

The case law discussed above demonstrates that the absence of a precise statute to combat computer crime can jeopardize the prosecution of criminal activity involving such sophisticated technology.[61] The federal prosecutor must seek conviction under statutes that were not designed to include computer crimes.[62] The outcome of the prosecution is then subject to the court's application of statutory requisites to computer abuse.[63] If the court fails to construe the statute liberally there will be instances where no federal criminal sanctions exist for

---

59. *See* United States v. Girard, 601 F.2d 69 (2d Cir.), *cert. denied*, 444 U.S. 871 (1979). In *Girard*, the defendants were charged and convicted under the theft and related offenses statute for the unauthorized conversion and sale of computerized Drug Enforcement Administration files. The Second Circuit upheld the conviction, interpreting the statute to include intangibles such as computer programs, computer time and computer printouts. *Id.* at 70-71. *See also* United States v. Sampson, [1978] 6 COMPUTER L. SERV. REP. 879 (CCH) (N.D. Cal. 1978), where the defendant was charged under the same statute. The defendant, a former NASA contractor, obtained unauthorized use of a United States government computer through his home telephone. The unauthorized use was discovered and, based upon defendant's statement that he used the computer for an average of six hours per week for thirty-two weeks, $1,924 was calculated as the amount of computer time he had stolen. *Id.* Defendant moved the district court to dismiss the indictment on the ground that it failed to state a criminal offense, arguing that computer time and storage capacity were not capable of being construed as property. *Id.* at 880. The district court denied the motion, finding that computer time and use of its storage capacities were "things of value." *Id.* at 881.

60. *See Computer Crime*, 19 AM. CRIM. L. REV. 499, 502 (1981) ("[t]he value of section 641 as a prosecutorial tool in computer related cases depends on whether a judge will interpret 'things of value' and 'property' broadly enough to include computer time and storage capacity"). *See, e.g.*, United States v. Lambert, 446 F. Supp. 890 (D. Conn. 1978) (defendants were charged under 18 U.S.C. § 641 for selling confidential information obtained from a computer within the Drug Enforcement Admistration). In *Lambert*, only the information, not the documents containing the information, was transferred. The defendants moved to dismiss, claiming that § 641 only applied to tangible items. The court denied the motion, holding that the statute is not restricted to the theft of tangible property and that the computerized records were "things of value" within the meaning of the statute. *Id.* at 895.

61. *See generally*, VOLGYES, *supra* note 4, at 398 (discusses result where there is lack of adequate statutes upon which to attack computer abuse).

62. *See supra* note 24; *see generally*, *Computer Crime*, 19 AM. CRIM. L. REV. 499, 506 (1981) (since computer crime offenses are charged under statutes not designed for computer use, failure to meet statutory requisites may result in acquittal).

63. *See* RODDY, *supra* note 2, at 356-57 ("[w]hen a statute is not specifically applicable, the decision to prosecute may be abrogated; when not abrogated, the court may feel constrained to find that the criminal activity is not within the reach of the law").

computer crime.[64] To remedy this deficiency, legislation prescribing penalties for illegal computer use should be enacted. Such legislation should be drafted to sufficiently define the wrongful activity,[65] deter future computer crime,[66] add certainty[67] and uniformity to these prosecutions,[68] and encourage reporting of such crime.[69]

B. Proposed Federal Legislation

Although no current federal statute specifically addresses computer crime, significant progress has occurred toward the enactment of such legislation. For several years, Congress has been considering The Proposed Federal Computer Systems Protection Act, which provides fines and imprisonment for violations.[70] This legislation was proposed in

---

64. *See* Gemignani *supra* note 57, at 706 for discussion of case where court had difficulty applying existing criminal laws to computer offense. *See generally* RODDY, *supra* note 2, at 352 (applicability of existing criminal statutes depends in large part on the particular circumstances of the crime; without statutory requisites fitting the particular circumstances, defendant may go free).

65. In order that wrongful computer abuse be sufficiently defined, effective federal legislation needs to specifically state the type of property it encompasses and to narrowly define the scope of the term "computer" as used within the legislation. See *infra* note 83 for a detailed discussion of the definition of the term "property" in the pending federal computer crime legislation. See *infra* note 78 for a discussion of the definition of the term "computer" in the pending federal bill.

66. Once computer crime legislation is enacted, many potential computer criminals will become aware of its existence and the Government's recognition of the wrongful activity, thus creating a deterrent effect. *See Hearings*, *supra* note 6, at 29; *see also infra* note 89 and accompanying text.

67. *See generally* COMPUTER CRIME, *supra* note 13, at 129; *Hearings*, *supra* note 6, at 11 (statement of Senator Ribicoff). Because of the lack of precise federal legislation, uncertainty surrounds the prosecution of a computer offense in that the prosecutor is forced to apply a statute written without computers in mind and to convince the court that all statutory requisites have been met. *See also supra* note 36 (discussion of difficulties prosecutors have in seeking conviction of a computer crime under existing penal laws).

68. Since computer crime is currently prosecuted under various federal statutes, it is subject to each statute's penalty limitations, which can result in an inappropriate punishment. *See generally* VOLGYES, *supra* note 4, at 400; *see also infra* note 85 and accompanying text.

69. *See generally* SOKOLIK, *supra* note 2, at 374 (an important benefit of computer crime legislation is that it will "encourage those who discover computer crimes to report and to cooperate in the prosecution of the perpetrators"). *See also infra* text accompanying note 159.

70. *See* COMPUTER CRIME AND SECURITY, *supra* note 12, at 4 (discusses history of congressional activity with respect to computer crime legislation). In 1977, Senator Ribicoff introduced S. 1766, The Federal Computer Systems Protection Act, 95th Cong., 1st Sess., 123 CONG. REC. 20, 953 (1977) [hereinafter cited as S. 1766]. An identical bill, H.R. 8421, was introduced in the House by Representative Rose and was referred to the Committee on the Judiciary. H.R. 8421 95th Cong., 1st Sess., 123

response to the deficiencies of existing laws, which do not contemplate computer abuse and cannot be effectively interpreted to accommodate this new form of illegal conduct.[71] Currently, H.R. 1092, The Federal Computer Systems Protection Act of 1983[72] is currently pending before Congress.[73] The bill proposes "[t]o amend Title 18, United

---

CONG. REC. 23,720 (1977). Hearings were held on S. 1766 before the Senate Committee on the Judiciary Subcommittee on Criminal Laws and Procedures. *Federal Computer Systems Protection Act: Hearings Before the Subcomm. on Criminal Laws and Procedure*, 95th Cong., 2d Sess. 1 (1978). The bill was never voted on by either branch of Congress. Senator Ribicoff reintroduced the bill in the 96th Congress as S. 240, The Federal Computer Systems Protection Act of 1979. 96th Cong., 1st Sess., 125 CONG. REC. 1190 (1979) [hereinafter cited as S. 240]. An identical bill, H.R. 6192, was introduced in the House by Representative Bill Nelson. 96th Cong., 1st Sess., 125 CONG. REC. 36,991 (1979). The Criminal Justice Subcommittee of the Senate Judiciary Committee held further hearings on S. 240. *See The Federal Computer Systems Protection Act of 1979 Before the Subcomm. on Criminal Justice of the Senate Judiciary Comm.*, 96th Cong., 2d Sess. 1 (1980). For extensive discussion of S. 240 *see generally* RODDY, *supra* note 2, at 349-52; Krieger, *Current and Proposed Computer Crime Legislation*, 2 COMPUTER L. J. 721, 724-27 (1980); Taber, *supra* note 23, at 517. These computer crime bills received no further action in the 96th Congress. When Senator Ribicoff retired in 1981, Representative Bill Nelson became the major force behind computer crime legislation. In the 97th Congress, Representative Nelson introduced H.R. 3970, The Federal Computer Systems Protection Act of 1981, which was referred to the House Judiciary Committee but received no further action. 97th Cong., 1st Sess., 127 CONG. REC. H3141 (daily ed. June 18, 1981). The 97th Congress also considered two other bills dealing with the safeguarding of computer information, H.R. 6420, Computer Software Piracy and Counterfeiting, 97th Cong., 2d Sess., 128 CONG. REC. H2359 (daily ed. May 19, 1982) (the bill's intent was to protect computer programs from duplication and illegal use), and H.R. 6006, 97th Cong., 2d Sess., 128 CONG. REC. H1341 (daily ed. March 31, 1982) (purpose of bill was to deal with computer security standards).

71. *See* COMPUTER CRIME, *supra* note 13, at 131.

72. The Proposed Federal Computer Systems Protection Act of 1983, H.R. 1092, 98th Cong., 1st Sess., 129 CONG. REC. H219 (daily ed. Jan. 31, 1983) [hereinafter cited as H.R. 1092].

73. H.R. 1092 is currently pending in the Civil and Constitutional Rights Subcommittee of the House Judiciary Committee. Telephone interview with Jim Southerland, Legislative Aide to Rep. Nelson (July 12, 1983). This Subcommittee held hearings on computer crime in September 1982, and anticipates further hearings on computer crime in 1983. Comments by Chairman Don Edwards (D. Cal.), *reprinted in*, COMPUTER CRIME AND SECURITY, *supra* note 12, at 5 (as of the date of this publication, the Hearing report had not been issued). Favorable House action is expected on H.R. 1092 this year. Telephone interview with Jim Southerland, Legislative Aide to Rep. Nelson (July 12, 1983). In addition, an identical bill, S. 1733, has been introduced in the Senate by Senator Paul Trible (R. Va.). Telephone interview with Stephanie Sears, Legislative Aide to Rep. Nelson (Aug. 25, 1983).

In addition to H.R. 1092, two other bills aimed at protecting computer use and security were introduced in the 98th Congress. *See* Small Business Computer Crime Prevention Act, H.R. 3075, 98th Cong., 1st Sess., 129 CONG. REC. H3144 (daily ed. May 19, 1983) (bill's intent is to encourage small businesses to protect their computer technology from criminal infiltration); Semiconductor Chip Protection Act of 1983,

States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce."[74]

H.R. 1092 consists of a preamble and four sections.[75] The preamble states that computer-related crime is a growing problem in both the government and private sector. In addition, such crimes are identified as being costly to the public. Many opportunities exist to commit these crimes, and prosecution under existing criminal statutes is difficult.[76] The purpose of this bill is to remedy the inadequacies in the present criminal code by proscribing as illegal certain computer conduct, such as (1) the introduction of fraudulent records into the computer system; (2) the unauthorized use of computer data; (3) the alteration or de-

---

H.R. 1028, 98th Cong., 1st Sess., 129 CONG. REC. H201 (daily ed. Jan. 27, 1983) (intent of bill is to protect semiconductor chips and masks against unauthorized duplication).

74. *See* H.R. 1092, *supra* note 72, at H219. H.R. 1092 describes the proscribed acts as follows: Subsection (a) of the bill defines as illegal any attempt to use a computer for fraudulent purposes or to embezzle, steal or knowingly convert another's property; penalties for violating section (a) are a fine of not more than two times the amount stolen or $50,000, whichever is higher, or not more than five years imprisonment, or both; Subsection (b) prohibits intentional, unauthorized damage, use, or alteration of a computer, computer programs, or stored information; the penalties for violating section (b), are a $50,000 fine or imprisonment of not more than five years, or both. In addition, Subsection (c) defines frequently used computer terminology, and Subsection (d) states that in a situation where federal jurisdiction exists concurrently with state or local jurisdiction, the existence of federal jurisdiction alone does not require its exercise. Although H.R. 1092 emphasizes federal computer systems in its title, its coverage goes beyond federal agency computers to those of financial institutions whose security is guaranteed by the federal government and to computer networks operating in interstate commerce or using interstate facilities. *See* NEWS RELEASE, *supra* note 2.

75. *See* H.R. 1092, *supra* note 72, at H219-20.

76. *Id.* at 219. The preamble to H.R. 1092 specifically states:

> (1) computer-related crime is a growing problem in the Government and in the private sector; (2) such crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime; (3) the opportunities for computer-related crimes in Federal programs, in financial institutions, and in computers which operate in or use a facility of interstate commerce through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great; (4) computer-related crime directed at computers which operate in or use a facility of interstate commerce has a direct effect on interstate commerce; and (5) the prosecution of persons engaged in computer-related crime is difficult under current Federal criminal statutes.

struction of stored computer data; and (4) the theft of financial instruments, data, or other assets.[77]

H.R. 1092 has the same title as previously proposed legislation[78] that was heavily criticized as unnecessary,[79] overbroad,[80] and containing excessive punishments.[81] The 1983 statute, however, has been extensively revised.[82] These revisions consist of rewording the definition of "computer" to provide a clearer statement of what constitutes wrongful activity within the context of the statute,[83] deletion of un-

---

77. *See* H.R. 1092, *supra* note 72 at H219. These categories are similar to the four types of computer crime discussed earlier. See *supra* note 76 for discussion of the four categories. See also *supra* notes 15-19 and accompanying text for specific examples of what type of activity is included in these categories.

78. *See supra* note 70.

79. *See* Taber, *supra* note 23, at 525-30. Taber claims that use of a computer does not create a unique crime, and that, thus, such crime is already adequately covered by existing criminal laws. *Id.* at 525. The validity of this proposition is doubtful. Taber fails to recognize the impact computer technology has had on traditional criminal statutes. These statutes are not easily adaptable to computer use because of the intangible aspects at the very center of computerization. Unauthorized computer use, misappropriation of computer programs, misuse of stored data, and computer time were clearly not anticipated when existing criminal statutes were drafted. The inability of present criminal laws to effectively curb computer crime is apparent. *See supra* note 36. Taber further argues that computer crime is not difficult to prosecute, noting that prosecutors have been able to obtain convictions under traditional criminal laws. Taber, *supra* note 23, at 528. To the contrary, although some prosecutions of computer abusers have been successful, they have not been easily secured by federal prosecutors. *See supra* notes 61-64. Absence of specific legislation has hampered the prosecutors' ability to prosecute. The need for precise legislation is obvious in order to avoid the possibility that the guilty may evade justice.

80. The criticism with respect to overbroadness was two-fold. First, it focused on the extremely general definition of "computer" as the statute was originally drafted, including computers used for personal, family, and household purposes. Second, it criticized the statutes' language as ambiguous with respect to precisely what actions it proscribed as wrongful computer use. *See generally* GEMIGNANI, *supra* note 57, at 709; RODDY, *supra* note 2, at 360-61.

81. Previously proposed bills were criticized for providing stiffer penalties and fines than the violations warranted. *See generally Hearings*, *supra* note 6, at 92-93; *Computer Crime*, 19 AM. CRIM. L. REV. 499, 505 (1981). Earlier bills provided for up to fifteen years imprisonment and fines of up to $50,000 for *any* computer violation; these penalties appear not to be directly proportional to the criminal activity. *See* S. 1766 and S. 240, *supra* note 70 ("whoever intentionally without authorization . . . attempts to damage or destroy any computer, . . . shall be fined not more than $50,000 or imprisoned not more than fifteen years, or both").

82. *See* NEWS RELEASE, *supra* note 2.

83. *See* H.R. 1092, *supra* note 72, at H219. In H.R. 1092, subsection 3(a), computer is defined as:

> [a]n electronic, magnetic, optical, hydraulic, organic or other high speed data processing device or system performing logical, arithmetic, or storage functions, and includes any property, data storage facility, or communica-

necessary computer jargon,[84] reduction in the prescribed penalties,[85] and the addition of a section giving the federal government concurrent jurisdiction with the states.[86]

Enactment of H.R. 1092 will have significant beneficial effects. It remedies the problems associated with the prosecution of computer crime cases by providing a specific statute under which to charge and seek conviction of a computer criminal.[87] The precisely worded definitions relieve uncertainty surrounding a court's determination of whether computer-related intangibles fall within the meaning of existing criminal statutes.[88] In addition, enactment of such legislation will

---

> tions facility directly related to or operating in conjunction with such device or system; but does not include an automated typewriter or typesetter, a portable hand-held calculator, or any computer designed and manufactured for, and which is used exclusively for, routine personal, family, or household purposes and which is not used to access, to communicate with, or to manipulate any other computer.

Compare this precise definition with the general definition of "computer" contained in S. 240, *supra* note 70.

> '[C]omputer' means an electronic device which performs logical, arithmetic, and memory functions by the manipulation 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.

84. The complex list of technological definitions included in earlier bills has been simplified. *Compare* the list of definitions in H.R. 1092, *supra* note 72, at H219-20, *with* the list contained in S. 240, *supra* note 70. For instance, the use of the noun "access" as a verb has been deleted, as have the terms "computer system," "computer program," and "computer software."

85. The penalties in previous legislation were clearly excessive and have been reduced. For penalties provided for in H.R. 1092, see *supra* note 74 and accompanying text. Drafters of H.R. 1092 appear to have followed the advice of their colleagues and have adopted penalties in direct relation to the amount of the gain derived, unlike the arbitrary fines contained in earlier bills. *See Hearings*, *supra* note 6, at 92-3 (statements of Senators Biden, Finney and Rohrbaugh) (Senator Rohrbaugh commented that the fine and prison sentence should be proportional to the amount taken by computer fraud or theft).

86. *See* H.R. 1092, *supra* note 72, at H220 section (d). Absent this provision, prosecutors utilizing a computer crime bill would have been faced with the difficulty of federal courts suddenly having jurisdiction over many activities which previously had been dealt with by the state courts. *See generally* RODDY, *supra* note 2, at 363; Comment, *Computer Crime—Senate Bill S. 240*, 10 MEM. ST. U.L. REV. 660, 667-68 (1980).

87. *See* NEWS RELEASE, *supra* note 2; *see generally* COMPUTER CRIME, *supra* note 13, at 129; Raysman, *Of Computers and the Law*, N.Y. Times, Sept. 14, 1980 § 3, at 18, col. 5. See also *supra* note 36 and accompanying text for a discussion of procedural and substantive problems encountered when seeking conviction of a computer criminal.

88. *See generally* RODDY, *supra* note 2, at 360. The detailed definition of "property" in the federal bill will relieve the courts of the difficulty inherent in interpreting

publicize the scope of illegal conduct and dramatize the punishment imposed.[89] Public awareness of the new federal computer crime legislation will deter potential abusers and encourage victims of computer crime and those who discover these crimes to report them immediately and to seek prosecution of the offender.[90]

III. State Level

A. Existing State Legislation

Although several states have enacted specific computer crime legislation,[91] the majority continue to rely on traditional state statutory law to combat computer crime.[92] State prosecutors encounter a degree of uncertainty, similar to federal prosecutors, as well as procedural and substantive impediments, when they charge a computer offense under criminal laws covering traditional offenses.[93] State prosecutors

---

the existent criminal code to include computer related offenses. "Property," as defined in H.R. 1092, *supra* note 72, at H219, subsection 3(a), covers "anything of value, and includes tangible and intangible personal property; information in the form of computer processed, produced, or stored data, information configured for use in a computer medium; information being processed, transmitted or stored; computer operating or applications programs; or services."

89. *See Hearings*, *supra* note 6, at 3. In introducing the federal computer crime bill, Senator Ribicoff stated that such legislation would deter the potential criminal and at the same time warn other white-collar criminals that their crimes will be dealt with in the most befitting manner. *See also* SOKOLIK, *supra* note 2, at 374.

90. See *supra* note 69 and accompanying text for a discussion of the benefit of public awareness of computer crime legislation.

91. *See* COMPUTER CRIME AND SECURITY, *supra* note 12, at 11. As of this date, computer crime legislation has been enacted in nineteen states. *See* ALASKA STAT. § 11.46.985 (1978); ARIZ. REV. STAT. ANN. §§ 13-2301, 13-2316 (West 1978 & Supp. 1982-1983); CAL. PENAL CODE § 502 (West Supp. 1983); COLO. REV. STAT. §§ 18-5.5101, 102 (Supp. 1982); DEL. CODE ANN. tit. 11, § 858 (Supp. 1982); FLA. STAT. ANN. §§ 815.00-.07 (West Supp. 1983); GA. CODE ANN. §§ 16-9-90-93 (1982); ILL. ANN. STAT. ch. 38, §§ 15-1, 16-9 (Smith-Hurd Supp. 1983-1984); MICH. COMP. LAWS ANN. §§ 752.791-.797 (West Supp. 1983-1984); MINN. STAT. ANN. §§ 609.87-.89 (West Supp. 1983); MO. ANN. STAT. §§ 569.093-.099 (Vernon Supp. 1983); MONT. CODE ANN. §§ 45-1-205, 45-2-101, 45-2-103, 45-1-104 (1981); N.M. STAT. ANN. §§ 30-16A-1-4 (Supp. 1983); N.C. GEN. STAT. §§ 14-453-457 (1981); OHIO CODE ANN. §§ 2901.01, 2913.01 (Page Supp. 1982); R.I. GEN. LAWS §§ 11-52-1.-4. (1981); UTAH CODE ANN. §§ 76-6-701-704 (Supp. 1981); VA. CODE § 18.2-98.1 (1982); WIS. STAT. ANN. § 943.70 (West Supp. 1982-1983).

92. *See* LEGISLATIVE RESOURCE MANUAL, *supra* note 1, at 1; *see also* COMPUTER CRIME, *supra* note 13, at 129.

93. *See generally* LEGISLATIVE RESOURCE MANUAL, *supra* note 1, at 1 (states have confronted difficulties in applying traditional criminal laws to situations involving use of computers); VOLGYES, *supra* note 4, at 400-01; see also *infra* notes 107, 110 and accompanying text for case law discussing present difficulty in prosecuting a computer criminal.

rely on eleven areas of law in computer crime cases.[94] These traditional areas, which vary widely from state to state, include laws against arson,[95] burglary,[96] embezzlement,[97] extortion,[98] forgery,[99] larceny,[100] criminal mischief,[101] receipt of stolen property,[102] theft,[103] theft of services or labor under false pretenses,[104] and theft of trade secrets.[105]

---

94. *See generally* LEGISLATIVE RESOURCE MANUAL, *supra* note 1, at 1-8; VOLGYES, *supra* note 4, at 400 (divides current state laws into ten areas). For a comprehensive study of existing state laws that may be applicable to combat computer crime, see Nycum, *The Criminal Law Aspects of Computer Abuse: Part I: State Penal Laws*, 5 RUTGERS J. OF COMPUTERS & L. 271 (1976).

95. In general, modern arson statutes refer to the malicious burning of a building. *See* LEGISLATIVE RESOURCE MANUAL, *supra* note 1, at 1. However, with respect to computers, arson may be charged where the computer is intentionally set on fire or where the computer tapes or programs are unlawfully burned. *Id.*

96. The common law statutory definition of burglary has been liberalized in that the definitions today require only an entry into any type of structure. *See* W. LAFAVE & A. SCOTT, JR., HANDBOOK ON CRIMINAL LAW 708 (1972) [hereinafter cited as LAFAVE]. Prosecution of a computer criminal under such a statute will be useful only if there was an unlawful entry into a computer facility, not if access had been gained into the computer data base in order to steal valuable information. *See* LEGISLATIVE RESOURCE MANUAL, *supra* note 1, at 3.

97. In general, embezzlement is defined as the fraudulent conversion of property belonging to another by one who lawfully possesses it. *See* LAFAVE, *supra* note 96, at 645.

98. The crime of extortion is generally charged to punish threats to do bodily harm, to injure property, to accuse the victim of crime, and to expose "disgraceful defect or secret of the victim." *Id.* at 705-06.

99. Forgery statutes may be successfully utilized to prosecute a computer criminal because the statutes have been modified to include the "making, altering, executing, completing or authenticating of any seal, signature, writing, or symbol of right, privilege or identification, that may defraud or injure another." *See* COMPUTER CRIME, *supra* note 13, at 136.

100. The crime of larceny is defined as the trespassory taking and carrying away of the personal property of another with intent to steal it. *See* LAFAVE, *supra* note 96, at 622. Seeking conviction for a computer crime under a larceny statute may be difficult depending on the statute's definition of "property" and "thing of value." *See* LEGISLATIVE RESOURCE MANUAL, *supra* note 1, at 3.

101. Criminal mischief is defined as "willful destruction of the property of another." *Id.* at 2. Since this statute generally requires tangible damage to property, problems exist in using such a statute to prosecute computer crime. *Id.*

102. Receipt of stolen property occurs when the receiver knows the property is stolen and intends to deprive the owner of his property. *See* LAFAVE, *supra* note 96, at 682-83.

103. Theft occurs when one misappropriates the property of another. *Id.* at 673. Because the statutes were originally designed with tangible property in mind, they may be ineffective against a computer offense.

104. Generally, theft under false pretenses occurs when the wrongdoer knows that he is making a false representation of a material fact and intends to defraud by causing the victim to pass title to his property to the wrongdoer. *Id.* at 655.

105. This offense occurs where a secret process or item used in a trade or business is unlawfully taken. *See* LEGISLATIVE RESOURCE MANUAL, *supra* note 1, at 4. Prosecu-

States have taken varying approaches in applying these statutes to computer crime. Some state prosecutors seeking conviction for a computer-assisted offense have relied on state courts to interpret existing criminal laws liberally to include computer crimes.[106] This approach has had limited success.[107] New York State has amended its penal laws to specifically include certain aspects of computer abuse.[108] Although

---

tion under this statute depends on fulfillment of the statutory requisites; consequently, since this type of statute requires a physical taking of property, it may be difficult to convict someone for theft of a computer program or stored data because of the property's intangibility. *See generally* COMPUTER CRIME, *supra* note 13, at 142; LEGISLATIVE RESOURCE MANUAL, *supra* note 1, at 4.

106. *See* Hancock v. Texas, 402 S.W.2d 906 (Tex. Crim. App. 1966), *aff'd sub nom.*, Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967) (affirmed defendant's felony conviction for theft of computer programs from employer). The defendant in *Hancock* contended that computer programs were not property within the meaning of the state statute. 402 S.W.2d at 908. The court rejected this argument and convicted defendant. Id. at 911. On petition for habeas corpus relief, the federal court held that the Texas court's construction of the state's theft statute did not violate federal due process. 379 F.2d at 553. *See generally,* People v. Gauer, 7 Ill. App.3d 512, 288 N.E.2d 24 (1972) (accuracy and reliability of telephone company's computerized records of telephone calls became an issue in case remanded for new trial).

107. *See* Ward v. Superior Court, 3 Comp. L. Serv. Rep. 206 (Cal. Super. Ct. 1972). Defendant Ward, an employee of a computer service company, acquired, through use of his employer's computer, a computer program belonging to a competitor. *Id.* Ward transferred the data by directing his employer's computer to transmit electronic impulses which represented the program. *Id.* He then had his employer's computer print the information onto paper. *Id.* at 207. Ward was charged under California's theft of trade secret statute. *Id.* However, the court noted that intangible magnetic impulses transferred from one computer to another did not constitute a trade secret absent a tangible copy. *Id.* at 208. Therefore, the court held that only the copying of the data was a violation under the statute. *Id.* Apparently, defendant was found guilty here solely because he had made copies of the program. *See also* Lund v. Commonwealth, 217 Va. 688, 232 S.E.2d 745 (1977) (computer time is not "goods or chattel" for purposes of Virginia state larceny statute requiring theft of property in excess of $100).

108. *See* New York's larceny statute, N.Y. PENAL LAW § 155.00(1) (McKinney 1975), which encompasses computer hardware and software, since it defines "property" as "money, personal property . . . or any article, substance or thing of value," and covers both tangibles and intangibles; New York's anti-tampering statute, N.Y. PENAL LAW §§ 145.15, 145.20, 145.25 (McKinney 1975), prohibits both tampering with any property that causes substantial inconvenience, and creating a risk of substantial damage to property, whether or not the damage actually occurs. Furthermore, part of New York's forgery statute, N.Y. PENAL LAW § 170.00(1)-(7) (McKinney 1975), defines forgeries to include symbols or identification. However, although New York's Penal Code includes certain categories into which certain computer related crime can be placed, there are statutes that are unclear in their scope. New York's theft of services law, N.Y. PENAL LAW § 165.15 (McKinney 1975), covers goods and services and other tangible things of value, but is unclear as to what degree intangibles would be covered. *See generally New York State Bar Association*, LEGISLATION REPORT ON COMPUTER CRIME 4, 16 (Oct. 22, 1982) [hereinafter cited as LEGISLATION REPORT] (New York's penal law can encompass many aspects of com-

this approach may appear sufficient, its success depends on the extensiveness of the states' penal codes.[109] While state prosecutors sometimes have been effective in obtaining convictions against computer criminals, neither of these approaches is totally satisfactory.[110]

B. State Computer Crime Statutes

Several states have demonstrated their concern with protecting computer systems and preventing computer crime through enactment

---

puter crime but there is need for specific state legislation to criminalize "unauthorized computer use" that is unique to computer technology).

109. For example, New York has amended several of its penal laws to permit conviction of a computer criminal. See *supra* note 108 for list of amendments to N.Y. Penal Code. It is important to note, however, that the New York Legislature is currently considering enactment of a specific computer crime bill. *See infra* note 123. Apparently, its purpose is to cover computer abuse that has not been reached by amending existing penal laws. *See generally* LEGISLATION REPORT, *supra* note 108, at 16.

110. For example, although New York has attempted to partially amend its penal code to reflect society's computerization, *see supra* note 108, there are still serious prosecutorial limitations on computer criminals who are apprehended. In People v. Weg, 113 Misc. 2d 1017, 450 N.Y.S.2d 957 (N.Y. Crim. Ct. 1982), the defendant, who had used his employer's computer for personal benefit, without authorization, was found not to have violated any law. The defendant, a computer specialist for the New York City Board of Education, had been charged with theft of services for unlawfully using the school system's computer to trace the geneology of horses he owned in order to further his winnings. *See* Haberman, *High-Tech Handicapper No Thief, Judge Says*, N.Y. Times, Apr. 25, 1982, at 51, col. 1. The court stated that the defendant had not broken any laws since (1) he had legitimate access to the computer and (2) the computer was not business, commercial or industrial equipment, as is required by the statute, but rather an administrative tool. 113 Misc. 2d at 1024, 450 N.Y.S.2d at 961. The court suggested that perhaps it was time for the New York State Legislature to enact specialized legislation to protect against new computer abuses. *Id.* at 1023-24, 450 N.Y.S.2d at 961. See also State v. Thommen, No. 79-424B (Ind. Crim. Ct. Marion Co. Feb. 14, 1980) which is discussed extensively in *Gemignani*, *supra* note 57, at 713-19. The defendant, a statistician with the Indiana Department of Mental Health, utilized his identification code to plug into his employer's computer and obtain highly confidential security programs in the main data base. *Id.* at 714. Since these programs had no relationship to Thommen's work, it was considered unauthorized access and the defendant was charged with theft of computer time. *Id.* at 715. The prosecutor, seeking an indictment and conviction faced potentially difficult procedural problems. *Id.* First, although it was impossible to ascertain whether defendant had taken any money because of the nature of the State's intricate computer system, the prosecutor chose to prosecute defendant for theft of computer time because defendant had confessed to use of the computer time. *Id.* at 715-16. Second, because defendant was charged under the State's existing theft statute, which requires that something of value must have been taken, the prosecution had to present extensive evidence that a valuable commodity had been taken. *Id.* at 716. Even though defendant argued that there was no law prohibiting his activity and that he had not deprived the State of anything, the jury was not convinced and found him guilty. *Id.* at 717. The case illustrates that computer crime can present difficul-

of explicit computer crime legislation.[111] Other states have drafted bills that are awaiting further action.[112] Apparently, state legislators have recognized the unique nature of computers and the deficiencies of current criminal laws.[113] Although each state computer crime statute is a unique complement to the state's penal code, a number of the enacted state computer crime statutes resemble earlier proposed federal legislation.[114] As a result, they suffer from many of the same inadequacies that were remedied in the federal bill by H.R. 1092.[115]

The main defect in these state statutes is that they contain the same broad definition of "computer" as do previous federal bills.[116] Another problem with some state computer crime statutes is that they infringe on areas already covered by existing state legislation, without specifying exactly which acts constitute crimes under the law and which do not.[117] Nevertheless, this defect can be easily remedied by drafting

---

ties beyond those encompassed by prevailing state criminal laws, such as valuing loss of computer time and computer programs in order to meet the statutory requisites.

111. See *supra* note 91 for list of enacted statutes.

112. In 1982, the following states considered computer crime legislation: Alaska, Delaware, Massachusetts, Minnesota, New York, and Oregon. *See* COMPUTER CRIME AND SECURITY, *supra* note 12, at 11.

113. As of the date of this publication, no prosecutions have been reported under these statutes. However, this is not an indication of the lack of necessity for such legislation. On the contrary, as the public becomes more aware of computer crime statutes, the benefits of the legislation will become apparent and use of the statutes will increase; no longer will there be a reluctance to formally report computer crime. See *supra* note 20, discussing reasons why there are few formally-reported computer crime cases.

114. *See generally* Becker, *The Trial of a Computer Crime*, 2 COMPUTER L.J. 441, 447 (1980) (earlier proposed federal computer crime legislation appears to have been the model for a significant number of state computer crime statutes). *Compare* S. 1766 and S. 240, *supra* note 70, *with* ARIZ. REV. STAT. ANN. §§ 12-2301, 13-2316 (West 1978 & Supp. 1982-1983); COLO. REV. STAT. §§ 18-5.5-101, 102 (Supp. 1982); MICH. COMP. LAWS ANN. §§ 752.791-.797 (West Supp. 1983-1984); N.M. STAT. ANN. §§ 30-16A-1-4 (Supp. 1983); and R.I. GEN. LAWS §§ 11-52-1.-.4 (1981).

115. See *supra* notes 79-81 and accompanying text for a discussion of these defects.

116. *Compare* the definition of computer, *supra* note 83, *with* statutes listed in *supra* note 114. Unlike H.R. 1092, the state statutes are not restrictive enough to exclude from their coverage automated typing equipment, a portable hand held calculator, or any computer used for personal, family, and household purposes. Hence, the public must rely on the discretion of state prosecutors to exclude these types of prosecutions.

117. *See, e.g.*, *Gemignani*, *supra* note 57, at 711; COMPUTER CRIME, *supra* note 13, at 129-133 (discussing overlap of state computer crime bills with state's existing criminal code; for example, where new computer crime statute defines same terms as existing statutes, courts will be faced with difficulty of determining precise definition). *Compare* ARIZ. REV. STAT. ANN. § 13-2301 (West 1978) *with* ARIZ. REV. STAT. ANN. § 13-1801 (West 1978) ("intent to . . . control property" spoken of differently in these two statutes; as a result, Arizona courts will be faced with making the determination).

statutes with language restricting coverage to new types of crime fostered by computers, such as unauthorized computer use,[118] rather than to traditional crimes committed with the aid of a computer.[119]

A further criticism of some existing state computer crime statutes is that they do not provide for graduated penalties.[120] Graduated penalties are appropriate for computer offenses because they deter abuse without requiring unreasonable punishment.[121] One commendable attribute of state statutes with graduated penalties is that, like their federal counterpart, their flexibility accommodates the rapidly expanding capabilities of computer technology.[122]

C. Proposed New York Computer Crime Legislation

Specific computer crime legislation was introduced in the New York State Legislature in 1983.[123] The proposed legislation would create an entirely new article of the penal code, Article 186, entitled "Unauthorized Computer Abuse."[124] The new legislation is directed at defin-

---

118. *See, e.g.*, State of New York Senate-Assembly, PROPOSED BILLS S.494, A.576, 1983-1984 REGULAR SESSION (Jan. 5, 1983) currently proposed New York computer crime bill, S. 494, and LEGISLATION REPORT, *supra* note 108, at 4, 16 (Legislation Report, in part, extensively comments on New York's proposed computer crime bill). Drafters of S. 494 recognized the potential for conflict between a computer crime statute and existing penal laws and, therefore, constructed a limited computer crime bill that could not be criticized for overbroadness or duplication. See *infra* text accompanying notes 141-42 for discussion of the advantages of a restrictive state statute.

119. See, e.g., *infra* text accompanying notes 125 & 136 for discussion of proposed New York State computer crime legislation.

120. *See, e.g.*, GA. CODE ANN. § 16-9-93 (1982); MINN. STAT. ANN. § 609.89 (West Supp. 1983); R.I. GEN. LAWS § 11-54-4 (1981); VA. CODE § 18.2-98.1 (1982).

121. *See Computer Crime—Senate Bill S. 240*, 10 MEM. ST. U. L. REV. 660, 666-67 (1980) (gives example of possibility of unreasonable punishment in absence of graduated penalties). Legislation providing for graduated penalties would "deter a computer programmer from stealing his employer's computer time without subjecting him to unreasonable punishment." *Id.*

122. *See Gemignani*, *supra* note 57, at 712 (commenting on what an ideal computer crime bill should contain).

123. On January 5, 1983, Senator Pisani introduced the bill into the Senate. It was promptly referred to the Committee on Codes. The identical bill was introduced into the Assembly by Assemblyman Murphy. It was also referred to the Committee on Codes. *See* State of New York Senate-Assembly, PROPOSED BILLS S. 494, A. 576, 1983-1984 REGULAR SESSION (Jan. 5, 1983) [hereinafter cited as S. 494]. Computer crime experts also have recognized that New York is in need of penal legislation to sufficiently combat computer crime. *See* LEGISLATION REPORT, *supra* note 108, at 1.

124. *See supra* note 123 at 1.

ing and averting the new types of crimes that are possible by abusing advancements in computer technology.[125]

The proposed New York legislation, S. 494, begins with a preamble which, using language similar to H.R. 1092,[126] asserts that crime involving computers is a growing problem in the State, both in the government and in the private sector. Further, the preamble states, the current penal laws should be amended to clearly and fully encompass such crime.[127] Unlike H.R. 1092, S. 494 prescribes three graduated classifications and penalties to reflect the seriousness of the proscribed behavior.[128] In addition, the bill defines several commonly used computer technology terms.[129] The bill concludes with proposed

---

125. *See* LEGISLATION REPORT, *supra* note 104, at 16. *See generally* Raysman and Brown, *Evolving Statutes on Computer Crime*, N.Y.L.J., Jan. 11, 1983, at 2, col. 4 (similar comments on earlier proposed computer crime bills in New York).

126. See *supra* note 76 and accompanying text for an extensive discussion of H.R. 1092.

127. *Compare* preamble of H.R. 1092, *supra* note 72 *with* preamble language of S. 494, *supra* note 123.

128. *See* LEGISLATION REPORT, *supra* note 108, at 20. *See also* S. 494, *supra* note 123 (unauthorized computer use is use of a computer without authority). S. 494 provides that:

> [a] person 'uses a computer' when he causes the computer to perform or to stop performing any operation [and] a person 'uses a computer without authority' when (a) the computer is utilized in the operation of a building or in or by any business, profession, occupation or educational, research or government facility; and (b) he knowingly and intentionally uses the computer (i) when he has no right or authority to do so or any reasonable ground to believe that he has such right or authority; or (ii) when he has previously received reasonable written notice that he has no right or authority to do so, even if he does have right or authority to use the computer in some other manner.

Id. at 2. Proposed Section 186.10, Unauthorized computer use in the third degree, prohibits any unauthorized use of a computer; violation of this section is a class B misdemeanor. A class B misdemeanor requires that the court impose a definite sentence, not to exceed three months. N.Y. PENAL LAW § 70.15 (McKinney 1975). Proposed Section 186.20 defines Unauthorized computer use in the second degree as use of a computer without authority with intent to commit another misdemeanor or to aid or conceal commission of such other crime. *See* S. 494, *supra* note 123. Such an offense is a class A misdemeanor. Conviction of a class A misdemeanor requires the court to impose a definite term of imprisonment, not to exceed one year. N.Y. PENAL LAW § 70.15(1) (McKinney 1975). Conviction under Section 186.30, Unauthorized computer use in the first degree, requires, in addition to unauthorized use, the intent to commit a felony or to aid or conceal its commission. *See* S. 494, *supra* note 123. Violation of this section is a class E felony, for which the jail term shall be fixed by the court, and shall not exceed four years. N.Y. PENAL LAW § 70.00 (2)(e) (McKinney 1975).

129. *See* S. 494, *supra* note 123. These terms include the following:

> (1) 'computer' means a device or group of devices which, pursuant to a computer program, can automatically perform arithmetic, logical, storage

amendments that would add violations for computer abuse[130] to the current New York penal laws for larceny,[131] theft of services,[132] and offenses involving false written statements.[133] As a result, these sections will address traditional crimes committed with computer involvement more effectively.

S. 494 is a modified version of the computer crime legislation introduced in the New York Legislature in 1982, but never enacted.[134] In its present form, S. 494 is effective state legislation that will amply cover criminal conduct committed with computer involvement. The primary difference between S. 494 and either H.R. 1092 or existing state computer crime statutes is that S. 494 is more limited in scope. Rather than extensively addressing computer fraud and denial or theft

---

> 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, another computer or another device the results of computer operations, computer programs or computer data; (2) 'computer data' means a representation of information, including the results of computer operation, which has been prepared with the intention that, in a suitable form, it be operated on by, or communicated to or from, a computer; (3) 'computer program' means a representation of one or more instructions . . . which, in a suitable form, can direct a computer to perform one or more operations.

Id. at 1-2.

130. *See* S. 494, *supra* note 123, at 2-4.

131. *See* N.Y. PENAL LAW § 155.00 (McKinney 1975). The proposed amendment would include computer data and computer programs within the meaning of "secret scientific material." It would define the term "computer service" and include it in the existing definition of "service."

132. N.Y. PENAL LAW § 165.15 (McKinney 1975). Proposed legislation would amend "theft of services" to include as a violation the attempt to avoid payment for computer time and, with the intent to obtain computer service, tampering with the equipment.

133. N.Y. PENAL LAW §§ 175.00, 175.20, 175.25 (McKinney 1975). Proposed legislation would amend the sections regarding falsifying business records and tampering with public records to include as violations the illegal use of computer data.

134. In 1982, two computer crime bills, S. 8310 and S. 8391, were introduced and considered by the New York State Legislature but never enacted. See Raysman & Brown, *Evolving Statutes on Computer Crime*, N.Y.L.J., Jan. 11, 1983, at 2, col. 4 for reference to these bills. These bills were modeled after the first federal computer crime bill. See *supra* note 114 and accompanying text for a list of such state statutes. Although the federal computer crime statute has undergone substantial modification from the original bill, *see* NEWS RELEASE, *supra* note 2, the proposed 1982 New York bills did not reflect these revisions. *See* LEGISLATION REPORT, *supra* note 108, at 2-3. The two bills were carefully scrutinized by computer law experts Walter Klasson, Esq. and Richard Raysman, Esq. who prepared an extensive report analyzing the shortcomings of the bills. The report concluded that the bills were overbroad, duplicative of existing New York penal sections and thus totally unacceptable. *Id.* at 1. Consequently, they proposed an alternative statute that has become the computer crime legislation currently pending in the legislature. *Id.* at A-1.

of computer services,[135] the drafters of S. 494 restricted its reach to prohibiting unauthorized computer use.[136] Although S. 494 is not as broad as is either the proposed federal bill or other state legislation directed at computer crime, this neither affects the bill's adaptability to future growth within the field of computer technology nor hinders the state prosecutor's ability to seek a conviction.[137]

The narrow approach of S. 494 is suitable for New York because the bill has been carefully drafted to work in conjunction with the existing penal code.[138] Since New York's penal code is extensive in its coverage of criminal activity,[139] it is unnecessary for New York to follow the lead of other states that have adopted broader computer crime statutes.[140] The advantages of a restrictive state statute are two-fold. First, it precisely defines the wrongful activity and cannot be criticized for overbroadness or ambiguity.[141] Second, there is no risk that the computer bill will overlap other penal laws, resulting in the need for courts to resolve the discrepancies.[142]

Unlike H.R. 1092 or previously proposed New York legislation, S. 494 provides graduated penalties and classifications of computer crime,[143] thereby avoiding the possibility of unreasonable penalties.[144]

---

135. *See, e.g.*, ARIZ. REV. STAT. ANN. §§ 13-2301, 13-2316 (West 1978 & Supp. 1982-1983) ("[a] person commits computer fraud . . . by accessing, altering, damaging, or destroying without authorization any computer, computer system, computer network . . . with the intent to devise or execute any scheme or artifice to defraud, deceive, or control property or services by means of false or fraudulent pretenses, representations or promises"); COLO. REV. STAT. § 18-5.5-101, 102 (Supp. 1982) (prescribes the knowing use of a computer for fraudulent purposes, the malicious destruction of a computer, and the unauthorized use or alteration of a computer or its data); FLA. STAT. ANN. §§ 815.00-.07 (West Supp. 1983) (prescribes offenses against intellectual property including data and programs, offenses against computer equipment and supplies, and offenses against computer users).

136. See *supra* note 128 and accompanying text for scope of S. 494.

137. A restrictive state computer crime bill does not jeopardize the state prosecutor's ability to obtain a conviction provided it was designed to complement the state's existing penal code; what is not within the reach of the limited computer crime legislation is covered by amendment of existing penal sections. See LEGISLATION REPORT, *supra* note 108, at 4, 16 for discussion of similar rationale underlying S. 494.

138. *See* LEGISLATION REPORT, *supra* note 108, at 4, 16.

139. *Id.* at 4.

140. See *supra* notes 114-16 and accompanying text for list of such statutes.

141. *See supra* note 80 and accompanying text (S. 494 is a more precise bill than is federal bill H.R. 1092).

142. See *supra* notes 108, 117 and accompanying text for discussion and examples of the risk of overlap.

143. On recommendation, the Legislature corrected the conflict with the pattern of New York's existing penal laws, which provide for graduated penalties, by providing for such penalties; in earlier proposed bills, all offenses were classified as felonies. *See* LEGISLATION REPORT, *supra* note 108, at 20.

144. See *supra* note 121 and accompanying text for an example of the possibility of unreasonable penalties.

A criticism of S. 494, however, is that the bill does not provide a penalty based on the value of use stolen or services stolen;[145] it simply prescribes varying misdemeanor and felony grade penalties.[146] Since the possibility for very costly crime exists, legislation should provide fines as an added deterrent.[147]

S. 494 improves earlier New York proposals by simplifying computer terminology used in the bill.[148] Computer crime legislation should not attempt to define in detail numerous aspects of computer terminology. Drafters of legislation regarding computer technology must be cautious in their use of technical terms because the terms do not have uniform definitions and are subject to judicial interpretations.[149] S. 494 does not suffer from an overbroad definition of "computer."[150] While not explicitly excluding computers used for hobbies and entertainment, the definition of "computer" in S. 494[151] limits the application of the statute to computers used in business, education and government.[152]

S. 494 reflects unique aspects of New York's penal code and recent developments in this area by the legislature.[153] The bill addresses the specialized problems raised by computers without unnecessarily infringing on areas already covered by existing legislation. S. 494 is

---

145. *See* LEGISLATION REPORT, *supra* note 108, at 19. Computer crime experts suggested that the New York Legislature add a felony grade of the crime based on the value of services stolen. *Id.*

See *supra* note 128 for discussion of penalty grades.

146. Several state computer crime statutes contain penalty provisions that relate directly to the value of the item stolen, or the loss or damage suffered. *See, e.g.*, CAL. PENAL CODE § 502(e) (West Supp. 1983); COLO. REV. STAT. § 18-5.5-102(3) (Supp. 1982); FLA. STAT. ANN. § 815.04 (West. Supp. 1983); ILL. ANN. STAT. ch. 38, § 16-9(c) (Smith-Hurd Supp. 1983-1984); MINN. STAT. ANN. §§ 609.88-.89 (West Supp. 1983); N.M. STAT. ANN. §§ 30-16A-3-4 (Supp. 1982); UTAH CODE ANN. § 76-6-703 (Supp. 1979).

147. *See* LEGISLATION REPORT, *supra* note 108, at 6-9. Previously considered computer crime bills, S. 8310 and S. 8391, included definitions of access, computer, computer network, computer system, computer program, computer software, financial instrument, property, services, intellectual property, and data. *Id.* See *infra* text accompanying note 148 for a discussion of the need for simplified terminology.

148. *See* Raysman & Brown, *Evolving Statutes on Computer Crime*, N.Y.L.J., Jan. 11, 1983, at 2, col. 1.

149. *See supra* notes 83, 116 and accompanying text.

150. See *supra* note 129 for definition of "computer."

151. *See* LEGISLATION REPORT, *supra* note 108, at A-1. In narrowing the scope of the legislation, proposers of S. 494 intentionally excluded from the legislation's reach computers used exclusively for personal purposes. *Id.*

152. *Id.* at 22.

153. See LEGISLATION REPORT, *supra* note 108, at 22 for a discussion of the unique aspects of the New York proposed computer crime legislation.

effective state legislation because it does not simply adopt statutory language from another jurisdiction.[154] Consequently, it did not inherit the deficiencies existent in earlier legislation.[155]

IV. Alternative for Legislative Action

There are three legislative alternatives with regard to computer crime. First, existing criminal laws can be left untouched, relying on the courts to liberally construe statutory requisites so as to include computer crime. Second, existing criminal laws can be amended to address certain aspects of computer abuse. Third, new, specific computer crime legislation can be drafted and enacted to effectively encompass such criminal activity.

Clearly, the first alternative, leaving existing criminal laws untouched, will not suffice on either the federal or state level. On the federal level, the third alternative, enactment of precise computer crime legislation, is needed to remedy the disagreement among district and circuit courts on whether certain existing federal statutes proscribe computer-assisted crime.[156] In addition, new legislation is needed to encourage reporting of such crime[157] to uniformly punish the offenders,[158] and to deter potential abusers.[159] The potential for computer abuse has been increasing steadily; H.R. 1092 is appropriate federal legislation to address such criminal abuse.[160]

It is apparent that present state procedures for dealing with computer crime are inadequate, as is their federal counterpart.[161] Application of traditional state criminal codes to computer abuse has created significant limitations and obstacles to effective prosecution. Existing

---

154. *See* Krieger, *Current and Proposed Computer Crime Legislation*, 2 COMPUTER L.J. 721 (1980) (complete text of existing and proposed legislation).

155. *See supra* notes 84-86 and accompanying text.

156. See *supra* notes 53 & 57 and accompanying text for examples of this disagreement.

157. See *supra* note 68 and accompanying text for problems associated with disparate penalty limitations.

158. See *supra* notes 66 & 89 and accompanying text for discussion of deterrent effect computer crime legislation will have.

159. *See supra* note 69 and accompanying text.

160. *See* Ingraham, *On Charging Computer Crime*, 2 COMPUTER L.J. 429 (1980) (argument that special recognition is not needed for computer crimes overlooks basic need for laws to proscribe certain types of conduct, as well as to enable the redress of wrongs).

161. See *supra* notes 93, 107, 110 and accompanying text for discussion of the ineffectiveness of the present state procedures.

state penal codes must be amended to encompass computer crime. On the state level, a combination of the second and third alternative is the most advantageous. Amendment of existing penal laws, the second alternative, may be sufficient to combat traditional crime that now occurs in a new computerized form.[162] This approach, however, varies with the adaptability of a state's existing penal code.[163] Even if states have extensive penal codes which can be amended in this way, the third alternative, enactment of precise computer crime legislation is needed to cover criminal conduct such as unauthorized computer use[164] that is specifically created by computer technology. Such legislation should be more limited in scope than is the proposed federal bill.[165] New York's S. 494 is an appropriate model for combining the second and third alternatives. Clearly, adequate legal redress on the state level is as imperative as is the corresponding need on the federal level.

V. Conclusion

Advancements in computerization and the growing use of computers in business, government, education, and the private sector[166] has resulted in the expanding potential for criminal infiltration. The problems of computer crime are in great part attributable to the shortcomings of our criminal laws and the reluctance of our legal establishments to change.

Wrongful computer activity was not envisioned when the current criminal laws were written. The difficulties in applying traditional

---

162. *See, e.g.*, LEGISLATION REPORT, *supra* note 108, at 4 (New York's penal laws broadly cover traditional criminal activity, into which many aspects of wrongful computer abuse can be placed).

163. A state's penal code can only be amended to the extent that it already proscribes the action as illegal. For instance, if a state does not have a law prohibiting theft of services, such law cannot be amended to prohibit the act committed with computer involvement. As a result, it will be more effective for the state to enact a broad new computer crime bill. *See* COMPUTER CRIME, *supra* note 13, at 129-131 (discussing such difficulties with Florida's penal laws).

164. *See, e.g., supra* note 109 and accompanying text (although New York has amended several of its categories of crime to include computer related offenses, experts still recognize the continuing need for a limited computer crime statute).

165. *See, e.g., supra* text accompanying notes 136 & 138 discussing New York's proposed computer crime bill.

166. In today's high technology world, computers are vital to our everyday lives. *See* NEWS RELEASE, *supra* note 2. It is estimated that six million American homes now have personal computers (micro-computers). *Id.* In the not too distant future, there will be a computer terminal on every desk and in every home.

laws to such activity are significant.[167] Beneficial and efficient use of computer technology requires that effective legislation be promptly enacted. The expansion of computer use will be followed by increasing levels of computer crime. Criminal laws for computer crime on both the federal and state level must be developed to curb these abuses.[168]

Elizabeth A. Glynn

---

167. *See supra* note 36 and accompanying text.

168. Pending the enactment of computer crime legislation, federal and state prosecutors will have to continue to rely on the present criminal codes with all their inadequacies and inconsistencies.