The John Marshall Journal of Information Technology & Privacy Law

Volume 2
Issue 1 *Computer/Law Journal - 1980*

Article 18

1980

The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review, 2 Computer L.J. 385 (1980)

Mary R. Volgyes

THE INVESTIGATION, PROSECUTION, AND PREVENTION OF COMPUTER CRIME: A STATE-OF-THE-ART REVIEW

By MARY R. VOLGYES*

INTRODUCTION

When computers were first introduced about thirty years ago, industry, business, and government were quick to grasp their enormous potential. At the same time, a number of equally enterprising individuals began to match their wits against the machines and learned to use them for criminal purposes. In the ensuing three decades, life in general, and crime in particular, have been radically changed by the computer.

For the man on the street, the computer revolution has generally meant new, faster, and better services. Computers automatically check out groceries, maintain up-to-the-minute balances in bank accounts, cash checks, and transfer funds or pay bills even when the bank is closed. They also assist in the diagnosis and treatment of disease and maintain records of social security and tax payments. Computers help local, state, and national governments in record-keeping, information retrieval, planning, budgeting, word processing, intelligence gathering, and complex research and analytical tasks. For business and industry, computers keep inventories, take care of billing, collections, and ordering, maintain

* A.B. 1960, Miami University. Ms. Volgyes is a widely published author whose works encompass a variety of social science disciplines. As senior staff writer, University Research Corporation, she participates in the firm's Law Enforcement Assistance Administration-funded programs to stimulate utilization of new findings from research in the criminal justice field. The author is indebted to Duane J. Gingerich, Esq., of Aspen Systems Corporation, for his analysis of federal and state statutes that apply to computer-related crime. Thanks also is due to Martha Collins, formerly of University Research Corporation, and now with *Science* magazine for research and editorial assistance.

mailing lists, predict marketing trends, plan and direct production, and handle many other vital operations.

Estimates vary, but one expert has suggested that more than 100,000 large-scale and 200,000 mini-computer systems were in use in the United States in 1978, and the total figure was expected to double by 1985.[1] A significant percentage of the gross national product is based on data processing and communications,[2] and virtually all of the nation's financial transactions are computerized, leaving the banking industry especially dependent on computers.[3] By 1985, when well over a half million computers may be operating worldwide, governments of most developed countries and virtually all large corporations will be reliant on computers.[4]

I. COMPUTERS: HIGH TECHNOLOGY FOR LOW RISK CRIME

In 1976, more than two million people—about three percent of the total United States labor force—worked with computers as programmers, operators, and maintenance technicians. Such people have access to systems that enable them to commit crimes. As the number of computers multiplies, so will the number of potential computer felons and the variety of their crimes. The computer has become a highly efficient tool for committing such crimes as fraud, embezzlement, theft, larceny, extortion, malicious mischief, espionage and sabotage.

Statistics gathered by the Federal Bureau of Investigation and other provide some notion of how effectively a computer assists the criminal. The average armed robbery nets about $9,000, and the average amount of funds reported missing from banks (including bank fraud and embezzlement) totals about $19,000, while the average computer fraud totals $450,000.[5] Newspaper headlines told of one of the largest schemes—a $10.2 million heist by computer at the Security Pacific Bank in Los Angeles. The infamous Equity Funding scheme, which used computers in a $2 billion fraud, is another example of how computers provide the technology that enables criminals to increase their "take" by many hundredfold. The annual cost of computer crime was pegged at $100 million by the United States Chamber of Commerce, but also estimated at $3.5 billion ac-

1. T. SCHABECK, COMPUTER CRIME INVESTIGATION MANUAL 1 (1979).

2. *Id.*

3. *Federal Computer Systems Protection Act: Hearings on S. 1766 Before the Subcomm. on Criminal Laws & Procedures, Senate Judiciary Comm.*, 95th Cong., 2d Sess. 3 (1978) (statement of Sen. Joseph R. Biden, Jr.) [hereinafter cited as *Hearings*].

4. *Id.* at 2.

5. T. SCHABECK, *supra* note 1, at 5.

cording to the Harvard Business Review.[6]

According to the Senate Subcommittee on Criminal Laws and Procedures, society, through the federal government, is also highly vulnerable to computer crime.

> The potential for defrauding the U.S. Government via computers is terrifying. The Department of Defense uses more than 3,000 computers. DOD, with the aid of some of these computers, disburses nearly $25 billion annually . . . . HEW computers generate $80 billion worth of checks each year. These check writing computers are not just hypothetical targets. In New York alone, doctors are thought to be overcharging HEW by $300 million annually.[7]

This vulnerability is expected to increase as new applications are found for the computer, as more people begin to understand and use computers, and as improvements in computer technology increase the complexity of systems. Modern life is becoming more and more vulnerable to the individual who can use the computer for criminal purposes, and crimes increasingly will involve their use. In the future, when electronic funds transfer systems usher in the predicted "cashless society," there will be even greater vulnerability to these high-yield, low-risk crimes.

> Traditional crimes may only be replaced by more sophisticated frauds. Paper trails may be nonexistent, and errors rampant. The prosecution of a felon who raises the defense of simple error is very difficult. Banking frauds may become highly lucrative for the felons of the future. With the assistance of a handful of insiders, criminals will be able to loot banks. Further, will stores with terminals in them be defined as bank branches? If not, then criminals may attack banks simply by making use of store terminals and thus, evade prosecution under many of the present federal bank statutes.[8]

A. High Yield-Low Risk Crime

Many experts categorize computer crime as a species of white-collar crime—*an illegal act characterized by deceit and concealment and not dependent on the direct application of physical force.*[9] However, this definition, that applies in instances in which the felon uses computer technology in the commission of a crime, does not include instances in which the computer itself is vandalized or destroyed. It is estimated that white-collar crime in this country

---

6. 125 CONG. REC. S711 (daily ed., Jan. 25, 1979) [hereinafter cited as CONG. REC.]

7. *Hearings, supra* note 3, at 3 (statement of Sen. Joseph R. Biden, Jr.).

8. *Id.* (quote from August Bequai in statement of Sen. Joseph R. Biden, Jr.).

9. GEN. ACCOUNTING OFF., REPORT BY THE COMPTROLLER GENERAL OF THE UNITED STATES, RESOURCES DEVOTED BY THE DEPARTMENT OF JUSTICE TO COMBAT WHITE-COLLAR CRIME AND PUBLIC CORRUPTION 4 (1979).

annually causes losses in excess of $40 billion.[10] Computer crime's actual share of this total is unknown, with estimates varying widely.[11] However, some believe that current projections of the scope of this technology-assisted crime represent just the tip of the iceberg.[12] Only an estimated fifteen percent of computer-related crime is reported.[13] According to FBI statistics, as of 1979, only 144 computer crimes had been reported to law enforcement agencies, and only 708 cases had been reported to any source.[14]

The reluctance to report computer crime is understandable, since publicity about such crimes can cause substantial embarrassment to businesses and governments. In fact, corporate executives apparently often prefer to cover up losses in order to prevent deterioration of public confidence, which could lead to a loss of business. Furthermore, public reports of such losses may only point up the vulnerabilities of computer systems to abuse through flaws that may not be remediable.

Even when guilty parties are detected, more often than not relatively little happens to them. Like white-collar criminals in general, computer criminals often receive minimal penalties.

> For example, the likelihood of going to prison for securities fraud in the federal system is 21.5 percent, and most sentences average only 20.5 months; it is only 19.5 percent for embezzlement, the average prison sentence being only 21.3 months; for postal embezzlement (mail fraud), the likelihood of going to prison is only 19 percent, the average sentence being 11.6 months. However, the likelihood of going to prison for crime classified as the "every-day type" by the government is 47.3 percent, the average prison sentence being 50.5 months.[15]

An FBI agent's study placed the chance of detection and prosecution at one out of twenty-two thousand.[16]

B. Categories of Computer Crime

Computer crimes are acts involving the use of information processing systems resulting in loss, damage, or injury. The General Account Office ("GAO") has offered one of the more comprehensive and useful definitions:

---

10. *Hearings, supra* note 3, at 2 (statement of Sen. Joseph R. Biden, Jr.).

11. CONG. REC., *supra* note 6, at S711. *See also* notes 5-6 *supra* and accompanying text.

12. *Hearings, supra* note 3, at 57 (statement of Donn B. Parker).

13. T. SCHABECK, *supra* note 1, at 4.

14. *Id.*

15. A. BEQUAI, COMPUTER CRIME 6 (1978) (footnotes omitted).

16. PROC. EDP AUDITOR'S ASS'N FOURTH ANN. FALL SEM. 10 (1977) (statement of FBI Special Agent B. Colvin).

> We define computer-related crimes as acts of intentionally caused losses to the Government or personal gains to individual related to the design, use, or operation of the systems in which they are committed. Computer-based data processing systems are comprised of more than the computer hardware and the programs (software) that run on them. The systems include the organizations and procedures—some manual—for preparing input to the computer and using output from it. Computer-related crimes may result from preparing false input to systems and misuse of output as well as more technically sophisticated crimes, such as altering computer programs.[17]

However, many other definitions have been put forward. According to a Congressional study, for example, the four main categories of computer crime are:

- introduction of fraudulent records or data into a computer system
- unauthorized use of computer-related facilities
- alteration or destruction of information or files
- theft, whether by electronic means or otherwise, of money, financial instruments, property services, or valuable data.[18]

Another classification puts most computer crimes into four somewhat difficult categories:

- sabotage and vandalism against a computer system itself
- theft of computer services
- property crimes (theft of property through the use of a computer)
- data crimes (theft of information, whether output data or intercepted data).[19]

These and most other definitions attempt to cover the diverse assortment of crimes that are computer-related. To understand their nature, it may be easier to follow Donn Parker's conceptualization, in which he considers crimes in relation to the four roles that computers play. "Every known case of computer abuse," he writes, "can be identified with one or more of these roles."[20]

The first role that computers can play in crime is to be the "object of the attack," in both planned assaults and irrational outbursts.[21] Computers have been shot, stabbed with a screwdriver,

17. GEN. ACCOUNTING OFF., COMPUTER-RELATED CRIMES IN FEDERAL PROGRAMS 1 (1976) [hereinafter cited as GAO REPORT].

18. CONG. REC., *supra* note 6, at S711.

19. A. BEQUAI, *supra* note 15, at 13-14.

20. D. PARKER, CRIME BY COMPUTER 17 (1976).

21. *Id.*

short-circuited with a car key inserted in a memory disc file, and damaged by bombing.[22] These crimes generally fit under the heading of vandalism, malicious mischief, and sabotage.

The second computer role in crime is that of "creating a unique environment in which unauthorized activities can occur, or where the computer creates unique forms of assets subject to abusive acts."[23] Crimes in this category have traditional names—theft, fraud, embezzlement, extortion, and so forth—but here they are associated with such developments as the increasing representation of assets in the form of magnetic patterns and electronic pulses stored in computers. Electronic funds transfer systems, which permit almost instantaneous bank account debiting and crediting, are a part of this unique environment. One bank embezzlement study showed that embezzlement by computer was four times more lucrative than more traditional embezzlement with average losses per case during the 1964-1975 period as less then $100,000, while computer-assisted embezzlement netted an average of $430,000.[24] Computer programs that have themselves become assets have been stolen.[25]

The third role of the computer is as the "instrument" of the crime.[26] Some ingenious crimes fall into this category. For example, using a computer to simulate, monitor, or track another crime program such as embezzlement or systematic burglary. Crimes in this category are also probably the most undetected and seldom prosecuted.

One example in this category is the case of a young man who took out a twelve-month installment loan from a New York bank. He received the loan and a book of computer-coded coupons to return with his installment payments. He paid only one installment, using the last coupon in the book, and received thanks in a computer-generated letter for paying off the loan promptly. The bank has since fixed the programming oversight, but the man was not prosecuted. In another case, a thief exploited the use by banks of the magnetic-ink character recognition imprinting system and devised a simple scheme that netted him $100,000. He took a stack of deposit slips from his bank, had his own account number printed on them in magnetic ink, and returned them to the trays in the bank. The computer sorted the deposits of all the people who used these

22. *Id.* at 18.
23. *Id.* at 19; emphasis omitted.
24. *Hearings, supra* note 3, at 57 (statement of Donn B. Parker).
25. D. PARKER, *supra* note 20, at 19.
26. *Id.* at 20.

slips and sent the money to the man's account. He withdrew his take before customers began to complain.

Fourth, computers are used "symbolically to intimidate, deceive, or defraud victims."[27] Attorneys, government agencies, and businesses, for instance, are increasingly using mounds of computer-generated data quite legally to confound their audiences. Criminals have also discovered the benefits of the imposing appearance of computer data. The phony invoice racket, an old mail-fraud scheme, is now assisted by computers that can churn out tremendous quantities of realistic looking bills relatively cheaply.

The General Accounting Office found in its 1976 study that although the same types of crime occur in the public, as well as the private, sector, computer-related crimes in government seem to involve proportionally more financial fraud and less vandalism and unauthorized use of services.[28] Another difference is that average losses are higher in private sector crimes.[29] The GAO studied sixty-nine cases in the federal government and found that sixty-two percent of those cases involved fraudulent input to computers.[30] Fraudulent input was used to tap supply systems, payroll, social welfare and compensation transactions.[31]

C. Technology to Control Technology

An obvious question is, why the computer cannot be used to protect against computer crime? Even though systems and safeguards are in place to minimize risks, the growing complexity of computer systems makes them increasingly vulnerable to a large variety of threats.

The first generation of computers processed jobs one at a time with input from a single source—a set of punched cards. The entire system was contained in a single facility. With no remote entry terminals, security was not difficult to ensure. Only a few people operated the machines, and what they were doing was readily apparent.

The second generation of computers had automated operator functions and multiprogramming capabilities that enabled them to handle more than one job at a time. Vulnerability began to increase. However, though it was more difficult to identify which job an operator was working on at any given time, the environment of the sys-

27. *Id.* at 21; emphasis omitted.
28. GAO REPORT, *supra* note 17, at 7.
29. *Id.*
30. *Id.* at 4.
31. *Id.*

tem was still local, and the operators were still a known and readily identifiable group.

The widely used, third generation machines have remote job entry capabilities which increased the system's vulnerability exponentially. Users are geographically dispersed, and systems are subject to wiretapping and unauthorized use. The most recent developments—remote interactive models of data management, time-sharing program development, and computer-to-computer networks—have introduced an even greater potential for crime. One computer can now be programmed to interact with another computer, introducing unfathomable technological capabilities for stealing or manipulating data or reprogramming computers for criminal purposes.

Control obviously involves a complex set of variables. Computer security specialists suggest a number of techniques, ranging from good management practices and proper screening of employees to physical protection of computer facilities. However, multiple users, dispersed access, and remote manipulation pose problems that lie outside of the sphere of conventional prevention and detection methods. Technology progresses faster than management can institute controls. It takes time to recognize the potential threats to a system and an even longer time to devise and institute safeguards. This time lag can be a major factor in permitting criminals to penetrate and use systems for their own ends.

Computer systems are shrouded by a mystique and an impersonality that enhances the intimidating effect of the technology. This effect is not restricted to people with little knowledge of how computers function; it extends to managers and top officials in corporations and government agencies that use computers extensively. According to one observer,

> [t]hese executive types seem to be fascinated by the efficiency of computers . . . and too often they tend to place in the veracity of these instant and apparently unassailable results, a faith that they would almost certainly hesitate to place in the work of mere human beings.[32]

Another factor complicating the issues of control and computer security is the psychological set of "man against machine" that pervades attitudes about computers. Though much of modern life is affected by and dependent upon computers, people often react negatively to what is perceived as the impersonality and dehumanization of this technology. In addition, since the computer is com-

32. Whiteside, *Annals of Crime: Dead Souls in the Computer*, 52 THE NEW YORKER, Aug. 22, 1977, at 35.

monly blamed for a variety of mistakes and human errors, people associate frustration with computer use.

II. THE COMPUTER FELON: WHITE-COLLAR, CLEAN HANDS, CLEAR CONSCIENCE

The impersonality of the computer and its environment tend to incite efforts to retaliate against the machine, and provide a rationalization for abusing it. "The computer lends an ideological cloak for the carrying out of criminal acts."[33] Computers also impart a clean quality to crime,[34] since overt violence is seldom involved. Computer crime also holds a variety of other attractions for potential criminals. For example, working out a formula that converts electronic assets into real money can be intellectually challenging, as well as difficult to detect.[35]

August Bequai described the "computer felon" as "young, educated, technically competent, and usually aggressive. Some steal for personal gain, others for the challenge, and still others because they are pawns in a larger scheme . . . . They are usually perceived as jovially challenging the machine, and discovery occurs only through inadvertence."[36]

In contrast to widely held opinions about the characteristics of computer criminals, the GAO study found that people with limited technical knowledge of computers, *e.g.*, key punchers, committed most of the crimes, rather than the programmers, operators, or analysts with more technical knowledge of the systems.[37]

In testimony presented to the Senate Subcommittee on Criminal Laws and Procedures in the summer of 1978, Donn Parker painted the emerging profile of the computer felon.[38] Most criminals in his study were between eighteen and thirty years of age, though there were a few older embezzlers in the ranks. They were highly motivated, intelligent, and often overqualified for their jobs. None took a particular job intending to engage in crime, and most had been on the job several years before any criminal attempt was made. Most perpetrated their acts in their own work environment, using their personal capabilities and positions of trust. The methods they used to attack the computer were generally unsophisticated. Most tended to excuse their acts by saying that they had not

33. *Id.* at 37.
34. *Id.*
35. *Id.*
36. A. BEQUAI, *supra* note 15, at 4.
37. GAO REPORT, *supra* note 17, at 4.
38. *Hearings, supra* note 3, at 58 (statement of Donn B. Parker).

harmed anyone, that those who were victimized deserved it, or that the attacks were aimed at organizations that could afford the losses. Job dissatisfaction rather than direct resentment of management was cited by most as a contributing factor.

Many sophisticated computer crimes are perpetrated by students and involve malicious mischief without serious financial loss. But, as Parker noted, "[t]here is some concern that students in data processing environments in universities have come to look on the computer as a game-playing device and do not treat it with the professional respect that a powerful tool deserves."[39] This notion may be one that is carried over into work and may result in greater computer abuses in the future.

On balance, four types of people are potential computer criminals: (1) *intruders*, or unauthorized users of a system; (2) *consumers*, authorized users of the output or products of a computer system; (3) *producers*, the programmers, analysts, and others who create the products or design the services; and (4) *servicers*, the keypunch or data entry clerks, maintenance personnel, and others who actually operate the information system.

III. Issues in Detection and Investigation

Detection of computer-related crime is hampered by the relative newness of the crimes, the absence of substantial case histories and other documentation, and the complexity of the technology involved. The problem is also compounded by the fact that some of those in a position to detect and report computer abuses—notably, accountants—feel obliged to respect the confidentiality of their clients, who do not want to be embarrassed by reports of penetration of their organization.[40]

Additionally, management may be unaware of how vulnerable their data processing operations are to criminal attack. Or, they may discover that some of the techniques and avenues that computer criminals use to penetrate their systems are not correctable or preventable. In some instances, managers may even reward the perpetrators of crimes with salary increases or promotions in an attempt to stop and hush-up the crimes.

Still another problem is the ease and speed with which fraud can be committed and camoflaged in the electronic data processing world. For example, the auditing of complex programs is so complicated that auditors often accept the computer output as accurate

39. *Id.*

40. D. Parker, *supra* note 20, at 15.

and only perform perfunctory audits. Auditors are also generally handicapped in detecting computer crime by a lack of training and experience in both data processing and criminal investigation.[41]

Many of the same problems that diminish the ability of auditors and managers to detect computer-related crime also hamper criminal investigators. These investigators must recognize the need to learn not only how to deal with a new environment of crime, but also how to work with unfamiliar groups of professionals—auditors, programmers and systems analysts—who may be the key figures in identifying crime or potential crime and assisting in the investigation.

A. Team Investigation

Though it is clear that the investigation of computer-related crime requires familiarity with electronic data processing, auditing, and accounting, investigators do not need to be computer experts. They do need to understand the system enough to use the knowledge of computer specialists in tracking possible crime. Police investigators must realize the necessity of cooperating with computer experts to ensure that they will obtain the type of evidence necessary to apprehend computer criminals.

Some businesses and government agencies have formed "fraud teams" to deal with the computer-related crime.[42] These teams may include criminal investigators, data processors, accountants and auditors. Whether a fraud team is available or whether investigators, auditors, accountants and data processors join in a less formal arrangement, a full investigation of suspected or detected computer abuse, if it is to result in prosecution, may require understanding of some or all of the following areas:

- documented types of computer-related crimes
- electronic data processing concepts and equipment
- nature of computer vulnerabilities
- investigative auditing, and
- applicable federal, state, and local laws.

B. Issues of Adjudication and Regulation

Though computer experts agree that prosecution of computer crimes must be bolstered, there is not even a consensus at present on what should be legally classified as a computer crime. Legal experts have begun generally to categorize these crimes in four broad

41. Schabeck, *Investigating Auditing*, ASSETS PROTECTION, Winter 1978, at 15.
42. *Id.*

classes, using Bequai's categorization[43]: sabotage and vandalism against the computer itself, property crimes (theft of property through the use of a computer), theft of computer services, and data crimes (theft of information, whether output data or the interception of data).[44]

Prosecutors face a great deal of uncertainty when they attempt to use traditional criminal statutes to prosecute such offenses. On the federal level, it has been estimated that there are as many as forty applicable statutes,[45] though none were specifically designed to address computer crime and abuses. Among federal statutes that may possibly be used are:

- mail fraud—essential elements of mail fraud are a scheme to defraud, use of the mails for purpose of executing the schemes, and intent to defraud[46];
- wire fraud—applies to schemes to defraud or obtain money or property by fraudulent pretenses through the use of "wire, radio or television communications" crossing state lines[47];
- embezzlement and theft—statutes only cover embezzlement or theft from agencies of the federal government and corporations in which the federal government has a proprietary interest[48];
- federal banking statutes—embezzlement or theft offender must be an employee, officer, or agent of a federally insured banking institution[49];
- malicious destruction or damage to federal government property—a broad reading of the required "injury" or "depredation" arguably may cover damage to government software[50];
- Omnibus Crime Control and Safe Streets Act of 1968—the elements of a Title III offense: interception of "oral communication," using electronic or mechanical devices, and involving interstate commerce[51];

---

43. *See* note 19 *supra* and accompanying text.

44. *Id.* at 14.

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

46. 18 U.S.C. § 1341 (1970).

47. *Id.* § 1343.

48. *Id.* §§ 641, 659.

49. *Id.* §§ 656, 657.

50. *Id.* § 1361. False entries into or alterations of the records (including bank computer records) of federally insured financial institutions likely would be covered under *id.* §§ 1005, 1006 (false bank entries, reports and transactions).

51. *Id.* § 2511. The use of a "spy" attachment to a computer in order to trace the

- arson—statute applies to arson in the context of "machinery, building materials, or supplies"[52];
- conspiracy—a criminal conspiracy involves agreement between two persons to commit a crime and an overt act in furtherance of that agreement[53];
- bank robbery—covers the taking of money or property belonging to federally insured banks or savings and loan associations "by force or violence"[54];
- national defense—statutes make it a felony to gather, transmit, or deliver defense information to aid a foreign agent or government[55];
- disclosure of confidential information—prohibits federal employees from making unauthorized disclosures of certain reports or records filed with the government[56]; and,
- interstate transportation of stolen goods and money—covers transportation, sale, or receipt of securities, fraudulent state tax stamps, and articles used in counterfeiting.[57]

Other federal statutes are indirectly related to computer crime control since they regulate the access to or disclosure of certain computer data. For example, the Trade Secrets Act[58] prohibits federal officials from disclosing confidential information to unauthorized persons. The Privacy Act of 1974[59] gives individuals certain safeguards against improper federal collection, storage and dissemination of personal information. The Federal Credit Reporting Act[60] imposes regulations on consumer reporting agencies regarding the confidentiality and use of acquired data.

C. Application of Federal Statutes

These statutes can be used with varying success to prosecute crimes involving computers. For instance, if a federal government computer facility is victimized by theft, the theft of government

---

location of unauthorized user of information stored in computer is not prohibited under this section. United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979).

52. 18 U.S.C. § 81 (1970).
53. *Id.* § 371.
54. *Id.* § 2113.
55. *Id.* §§ 793, 794.
56. *Id.* § 1905.
57. *Id.* §§ 2414, 2315.
58. *Id.* § 1905.
59. 5 U.S.C. § 552 (1970).
60. 15 U.S.C. § 1681 (1970).

property statute can be used and "is broad enough to cover both computer programs and services."[61] The statute prohibiting the destruction of or damage to government property "has been construed broadly and should include injury to software."[62] Both the wire fraud and mail fraud statutes can be used "for perpetrations of fraud involving the media."[63] The latter two have also been used more broadly in computer-related crime prosecutions and have been interpreted by the courts to fit many situations involving computer manipulation.[64] In addition, according to Susan Nycum:

> Acts of theft of and damage to physical aspects of computer systems as such—that is the equipment and supplies—present no new legal issues. Such items are tangible personal property and common law in the state and federal jurisdictions.[65]

As Susan Nycum pointed out during the Senate hearings on S. 240: "[n]otably absent"[66] from any list, however, are sanctions in federal or state statutes covering the unauthorized transferrence of electronic impulses, a particularly troublesome "loophole" considering the growing use of electronic funds transfer systems as well as the accessibility of confidential information of all sorts to skilled computer programmers and operators.[67]

The lack of statutes to attack computer abuse can jeopardize the prosecution of sophisticated computer fraud. A recent case illustrates the problem well.[68] A former employee of a Maryland computer firm—Seidlitz—was siphoning services from his past employer's computer, which provided data processing services to the Federal Energy Administration. Seidlitz gained access to the computer via telephone from his Maryland home and his Virginia office and stole a valuable and confidential program. Maryland and Virginia prosecutors were unsuccessful in using the statute dealing with the interstate transportation of stolen property.[69] Apparently, the movement of magnetic impulses from the victim's computer in Maryland to the defendant's computer in Virginia did not satisfy the

---

61. *Hearings, supra* note 3, at 71 (statement of Susan H. Nycum).

62. *Id.* at 28 (statement of John C. Keeney, Deputy Ass't Att'y Gen., Crim. Div., Dep't of Justice).

63. *Id.*

64. *See, e.g.*, United States v. Seidlitz, 589 F.2d 152, 7 CLSR 22 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979).

65. *Hearings, supra* note 3, at 70 (statement of Susan H. Nycum).

66. *Id.* at 71.

67. *Id.*

68. United States v. Seidlitz, 589 F.2d 152, 7 CLSR 22 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979), *discussed at Hearings, supra* note 3, at 28 (statement of John C. Keeney).

69. *Id.* at 29.

traditional interpretations of "stealing" or "taking," and "property," as required by the statute.[70] Seidlitz, however, did use interstate wire signals on several occasions and was charged and convicted under the federal wire fraud statute.[71] The statute was applicable only because Seidlitz placed two of approximately forty telephone calls to the Maryland firm from his office in Virginia.[72]

Where state and local prosecutors have no mail or wire fraud statute comparable to federal law, prosecution of computer theft may be extremely difficult or impossible. The interpretation of whether acts of theft and damage to computer programs are crimes varies widely from state to state. The answer often hinges on whether a computer program is considered property under a state's statutes or case law. The Maryland common law concepts of property theft, for example, did not readily apply to computer programs.[73] Thus, if Seidlitz had not used interstate telephone lines, he might have been found not to have committed a crime at all under Maryland law.[74]

Some states now have laws which specifically define computer programs as property[75]; but where the actual monetary value of the programs is not clear, the theft of a program may well be considered only a misdemeanor, despite the potential seriousness of the crime. Similar problems in state law arise in relation to the alteration and destruction of computer programs.

D. The Legislative Horizon

Though no current federal statutes specifically address computer crime, there is legislation now before Congress which would remedy that situation.[76] S. 240 proposes "to amend Title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes any computer owned or operated by the United States,

---

70. *Id.*

71. 18 U.S.C. § 1343 (1970).

72. *Hearings, supra* note 3, at 29 (statement of John C. Keeney).

73. A 1979 amendment, however, inserted the terms "computer software and programs in either machine or human readable form" as part of the definition of "property." MD. CRIM. LAW § 340 (Supp. 1979). *Hearings, supra* note 3, at 29 (statement of John C. Keeney).

74. *Id.*

75. *See, e.g.*, FLA. STAT. ANN. § 815.03 (West Supp. 1979).

76. 125 CONG. REC. S711 (daily ed., Jan. 25, 1979). The bill, S. 240, 96th Cong., 1st Sess. (1979), is entitled "Federal Computer Systems Protection Act of 1979." A virtually identical bill, S. 1766 was introduced by Sen. Ribicoff in the ninety-fifth Congress (*see* 123 CONG. REC. 10,790 (daily ed., June 27, 1977)), but failed to be reported out of the Senate Committee on the Judiciary before the end of the second session. The Senate Judiciary Committee held hearings on S. 240 on February 28, 1980.

certain financial institutions, and entities affecting interstate commerce." A rapidly growing number of states have already addressed the problem of computer crime through specific legislation.[77]

E. Enforcement at the State Level

The majority of state jurisdictions must still rely on traditional criminal law concepts to combat computer crime. Laws against arson and burglary, for example, can be used in some cases involving the destruction of property housing the computer system or breaking and entering into computer facilities to destroy valuable programs.

In addition to numerous laws against theft of property, the common law and statutory crimes of larceny, embezzlement, false pretenses, extortion, malicious mischief, forgery, and receiving stolen property have a direct bearing on computer crime control in those states that have no specific legislation on computer crime. The laws on these crimes, formulated long before computers existed, have their own procedural and substantive problems and peculiarities when applied to computer crime cases.

F. Adapting Existing Laws

Because of the multistate and interstate nature of computer operations, and especially because of developing computer networks, uniform state legislation on computer-related crime would be most effective. Since achieving uniformity in state laws is unlikely, however, federal law may be essential, especially in cases where the interpretation depends on facts, concepts, and evidence that are themselves so dependent on technology.[78]

Drafting specific legislation poses its own problems, again because of the highly technical nature of the subject matter. As computers have taken over what were once transactions directly between people, the type of evidence required in the prosecution of computer crimes has moved into the realm of electronic impulses and computer-kept records. If the law addresses computer crime by attempting to define each minute detail surrounding the use of this new type of evidence, prosecutors are likely to find themselves confronting gap after gap as new aspects of computer use and misuse

77. *See, e.g.*, FLA. STAT. ANN. § 76-6-701 *et seq.* (West Supp. 1979); N.C. GEN. STAT. § 14-453 *et seq.* (Supp. 1979); CAL. PENAL CODE § 502 (Supp. 1980); ILL. REV. STAT. § 81-548 (1980); N.M. STAT. ANN. § 30-16A-1 *et seq.* (Supp. 1980).

78. *Hearings, supra* note 3, at 71 (statement of Susan H. Nycum).

develop.[79]

The law must adapt to the changes, however, and the imaginative use of existing and developing statutes by prosecutors well versed in electronic data processing can help to develop appropriate methods of dealing with the trail of computer evidence.

VI. CONCLUSION

Though the data processing industry concedes that the detection of computer-related crime is difficult, even with the help of auditors, it is also acknowledged that law enforcement and management have not adequately used and exchanged the information currently at their disposal. Most computers in operation today were designed before the security issue was fully recognized. There are still no formal security criteria to guide designers, and security problems increase as the size of the systems and interconnections grow. The need to share computer hardware, data, and communications further complicates the security problem.

There are responses, many of which have long been recognized, and basic management controls that can help guard against computer misuse. The GAO report spelled out four ingredients needed to develop satisfactory internal controls:

1. An organizational plan that segregates duties of individuals to minimize opportunities for misuse or misappropriation of the entity's resources.
2. A system of authorization and record procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenses.
3. An established system of practices to be followed for each duty and function of the organizational departments.
4. An effective system of internal review.[80]

Further, the GAO noted that the most common weaknesses exploited by computer criminals in the federal agency cases it studied were in "(1) separation of duties and (2) physical control over facilities and supplies."[81] The annals of computer crime nationwide suggest that these two weaknesses are also widely exploited elsewhere. However, both are vulnerabilities that can be overcome.

Pointing out the high incidence of collusion in computer crime, Parker cites "journaling, monitoring, separation of responsibilities,

79. *See, e.g.*, Tapper, *Evidence from Computers*, 8 GA. L. REV. 562 (1974), *reprinted in* 4 RUTGERS J. COMPUTERS & L. 324 (1975).

80. GAO REPORT, *supra* note 17, at 9.

81. *Id.*

and dual controls over work activities of the employees,"[82] as the most effective measures.

Technology does exist that can reduce computer crime. The essential knowledge, however, is dispersed among a number of disciplines and in the works of a few experts throughout the country. As in many new fields, the experts, for the most part, talk to other specialists; and the average system user—the vulnerable businesses and governmental agencies that depend so heavily on the computer—often do not fully recognize the problems. In cases where realization has come, it has frequently come as a result of losses sustained through computer crime. Generally, the vulnerable system user has no idea where to turn for help before problems develop.

The challenge then is to devise means to disseminate the available knowledge and promote awareness of the problem. Computer crime can be reduced. But effective solutions will require that the user community be informed about the extent of their vulnerability, and those with knowledge of the problem help users implement practical techniques for detection, investigation, prosecution, and most importantly, prevention.

82. *Hearings, supra* note 3, at 58 (statement of Donn B. Parker).