
Stanley L. Sokolik

Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

http://repository.jmls.edu/jitpl/vol2/iss1/17

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
COMPUTER CRIME—THE NEED FOR DETERRENT LEGISLATION†

By Stanley L. Sokolik*

TABLE OF CONTENTS

I. THE GROWING DEPENDENCY UPON THE COMPUTER ....... 354
   A. Beneficient Explosion of Computer Technology ...... 354
   B. Pervasiveness of Computer Applications ............. 355
   C. Cashless/Checkless Society .......................... 357

II. COMPUTERS AND CRIME ...................................... 358
    A. Awesome Opportunity for Crime .................... 358
    B. Technological Lag in Computer Security .......... 361
    C. Modernizing Crime or Committing New Crimes? ..... 361
    D. Kinds of Computer Crime ............................ 363

III. COMPUTERS AND CRIMINALS ................................. 365
     A. General Profile of the Computer Criminal .......... 365
     B. Segments Within the Known Perpetrators .......... 366
     C. Motivational Influences Leading to Computer Crime 367

IV. DEALING WITH THE PROBLEM OF COMPUTER CRIME ........... 368
     A. Crime Deterrence Through Improved Computer Security 368
     B. Punishing the Computer Criminal .................. 371
     C. Role of Computer Crime Legislation ............... 373

V. ALTERNATIVES FOR LEGISLATIVE ACTION ................... 375
    A. Prosecution Under Existing Laws ................... 375
    B. Federal Computer Systems Protection Act .......... 378
    C. Emerging State Legislation ........................ 381

VI. CONCLUSION ................................................ 382

† This article is based on a report submitted by the author to the Data Information Systems Commission of the Illinois General Assembly in 1979.

* B.S.B.A & M.B.A., Washington University, St. Louis, Missouri; Ph.D, Ohio State University, Columbus, Ohio. Mr. Sokolik is currently President of Stanley L. Sokolik & Associates, a management consulting firm specializing in computer systems for management, project management, management and organizational planning, and personnel administration.
I. THE GROWING DEPENDENCY UPON THE COMPUTER

Today, only thirty-four years after the development of the first electronic computer, there is no person or organization that is not affected by the use of this invention. For all larger organizations and for many smaller ones, the computer has become the single, most important tool in their business. The computer is indisputably the means for, and the bane of, today's yearning for more, and more rapidly processed, information. It has demonstrably changed the behavior of all human beings, both at work and at leisure, and has made them more and more dependent upon its correct and reliable performance.

A. Beneficient Explosion of Computer Technology

The electronic computer has been in existence during only a very small part of recorded history. Indeed, it was as recent as 1946 that the first machine, the "Electronic Numerical Integrator and Calculator" ("ENIAC"), came into existence at the University of Pennsylvania.1 This original computer contained eighteen thousand vacuum tubes and carried out five thousand additions per second. Though the ENIAC was an astonishing success, today's computers use tiny silicon chips and perform millions of computations per second. They store tens of thousands of bits of information on miniscule electronic components measuring no more than one-quarter of an inch square.

In a national survey conducted in 1971 by Time magazine and the American Federation of Information Processing Societies ("AFIPS"), forty-nine percent of the participants reported that their jobs required direct or indirect contact with a computer.2 More recently, AFIPS projected that over sixty percent of the United States labor force will depend, in some way, on electronic data processing by 1990.3 AFIPS has estimated that there will be a doubling in the industry's volume every five years through 1990.4 Total user spending on data processing in the United States is expected to rise from 2.1% of the gross national product in 1970, to 13% in 1990, and from

---

4. Id. at 4.
$100 per capita to $1,253 per capita during these same twenty years.\textsuperscript{5} In 1976, the federal government alone was reported to have over nine thousand computers and to have expended more than $10 billion to procure and operate them.\textsuperscript{6}

The electronics company expected by many to dominate the personal (home) computer market announced in 1978 that its initial entry into that field would be a $300-$400, typewriter-size console that would use any home TV set for its video display.\textsuperscript{7} A peripheral product was designed to permit the user to “talk” by telephone to other computers.\textsuperscript{8} A $3 billion annual market for home computers has been projected for the early 1980s.\textsuperscript{9} In addressing a 1977 industry-wide conference, the chairman and chief executive officer of this company said, “[t]he remarkable fact is that in computing technology . . . we stand today at the midpoint of a 12 order-of-magnitude change in the nature of the computing world.”\textsuperscript{10}

B. Pervasiveness of Computer Applications

The mounting numbers of computers, and workers involved in their use, give ample testimony to their spreading presence and utilization throughout the American workplace. Far from remaining a scientific curiosity, the computer has moved out of the laboratory and into every conceivable industrial and government setting, as well as into a myriad offices operated by organizations of all kinds. The computer has become the workhorse of information processing generally. With the advent of the capability for concurrently sharing a computer's time, the number of users and uses is no longer bounded by physical space. Today, there is no turning back. Society could not revert to the days of manual processing of information even if it wanted to do so.

The computer has given rise to, and has made economically possible, countless opportunities for business, not-for-profit, and governmental endeavors. Most of these have come to fruition with far less cost and with much improved decision-making than would have been possible without the computer. Today, these organizations

\textsuperscript{5} Id.
\textsuperscript{6} COMPTROLLER GEN., MANAGERS NEED TO PROVIDE BETTER PROTECTION FOR FEDERAL ADP FACILITIES 3, 5 (1976).
\textsuperscript{7} Texas Instruments Shows U.S. Business How to Survive in the 1980s, BUS. WEEK, Sept. 18, 1978, at 90.
\textsuperscript{8} Id.
\textsuperscript{9} Id. at 92.
\textsuperscript{10} McCarter, Where is the Industry Going?, 24 DATAMATION, Feb. 1, 1978, at 107 (statement of Mark Shepard, Jr., then Chairman and Chief Executive Officer of Texas Instruments, Inc.).
could not survive without their computers. Their information-dominated world is too large, complex and vulnerable to manage and operate without these machines.

The magnitude of uses to which computers are applied, and the volumes of information processed by them, have created a growing dependence upon them—a dependence on the part of those who use them, as well as of those whom they serve. Furthermore, as their uses become more widespread, and technological developments increase access still further, this dependence will continue to grow.

To some degree, the manner in which computer usage has developed has added to user vulnerability. Generally, the economics of computers have led users to go beyond merely combining the different uses which initially justified their installation. Larger users have centralized their information processing, thereby creating an even greater susceptibility to catastrophic losses. The very virtue of the computer, its ability to store and manipulate large amounts of data has made it a ready tool for crime. Access to computers has been made available to more and more of the general population. At the same time, the increasingly complex technology of today's computers depend upon an exceedingly small number of individuals with highly specialized insights, knowledge, skills and motivations for their development.

Even as this article was being prepared, there were new indications of continuing technological progress within the electronics industry. The largest United States computer manufacturer announced substantial innovations resulting from what it saw as its "leading edge" of research.\(^\text{11}\) Far more than simply refinements of existing design, its new computers make use of "large scale integration" in both the memory and logic components, to better meet the needs of both "new customers and the most sophisticated ones."\(^\text{12}\) This new technology will again lower the threshold for implementing new data processing applications, provide over twice the memory and process information four times as fast as the previous comparable system, all at a significantly lower price.\(^\text{13}\)

While there has been a general doubling of consumer prices in the United States during the past twenty-five years, innovations of this one manufacturer have reduced the per-computation costs of its computers by 180 times during the same period.\(^\text{14}\) In just two years,


\(^{12}\) More Technological Advances [IBM Advertisement], Bus. Week, Mar. 5, 1979, at 68.

\(^{13}\) Id.

\(^{14}\) IBM 1978 Annual Report, supra note 11, at 5.
1977 and 1978, the price of memory in its major computers was cut by five-sixths.  

The result of this short, but rich, history of the electronic computer is that the fortunes of banks and other financial institutions, public utilities, larger not-for-profit endeavors, the federal, state and local governments, and large corporations of all kinds are irretrievably entwined with their computers and computer personnel. In similar fashion, the well-being and, at times, physical security of all citizens are tied to the functioning of computers. The responses to the Time Survey attest to the public's acceptance of both of these conclusions: eighty-nine percent of the participants agreed that (1) many things done by businesses would be impossible without computers and (2) computers provide beneficial information and services to them in their roles as consumers.  

C. Cashless/Checkless Society

One of the most complete displacements of manual methods by computer technology is in the electronic transfer of funds ("EFT") between individuals, financial institutions and retail stores. EFT substitutes the transmission of electronic impulses for money and checks. All that is necessary to pay for merchandise, make a deposit, withdraw funds, or pay a bill under EFT is the activation of a computer with a specially prepared card and "Personal Identification Number," or sometimes just by dialing a special number on a telephone. The technology is available now—both to make EFT possible and to exploit it for criminal purposes.

EFT exposes more of the general population to the impact that computer technology is having on the nature of work and forms of information. Now, more than ever, individuals are finding it necessary to use a terminal keyboard, read a cathode ray tube ("CRT") and interact with a distant computer. They are reassured by the realization that some of the criminal risks that they have faced in the past—theft, mugging for gain, and forgery—will no longer be as common. Yet, they cannot help but worry about computer criminals and the large sums that they may be able to take from the account balances that are recorded only in distant computers.

While EFT is not free from the risk of wiretapping given available technology, the use of microwave transmission is nevertheless seen as eventually linking a nationwide system of some forty million terminals and thousands of EFT computers. The annual volume of checks—forty billion by 1980 in the United States alone—and a cost

15. Id.
16. TIME SURVEY, supra note 2, at 4 & 35.
of more than $8 billion annually for processing them almost guarantee that available computer technology will be used to develop a wide-ranging EFT system.

II. COMPUTERS AND CRIME

Growing dependence upon the computer has created a serious economic, social and political problem: dealing with crimes involving computers and their data. The problem has developed at a rate which can only be likened to that of advances in computer technology itself. It is also a problem as limitless as the technology which spawned it. What has only recently been regarded as the "crime of the future" is today acknowledged by many as already here.17

A. Awesome Opportunity for Crime

The number of computers, the number, complexity and significance of their applications, the number of persons directly involved in their use, the amount of data concentrated in individual computer facilities, and the economic value of the information processed, all increase the opportunity and likelihood of worthwhile payoffs from computer-related crimes. Furthermore, the vulnerability of most computer systems makes the payoffs appear possible without much risk of detection and, oftentimes, without any evidence that a crime has occurred.

The backdrop and potential of computer crime was convincingly set forth in the testimony of John C. Keeney, then acting United States Assistant Attorney General for the Criminal Division, before the Senate Subcommittee on Criminal Laws and Procedures:

Our political, economic and social institutions have grown increasingly dependent upon computers to the point that their illicit manipulation or malicious destruction can potentially wreak havoc on society. Consider in this regard the consequences resulting from the willful destruction of the computer-generated social security checks flowing to the elderly or disabled, the destruction of a bank's computer records of its demand deposits, or the malicious destruction of irreplaceable medical research data stored in a computer bank. Computers have become a part of everyone's life and are being integrated into virtually every facet of human activity at an ever increasing rate. The very existence at the present time of a broad base of computer usage and computer knowledge, and its projected increase in the years to come, suggests that we will experience an

increase in the opportunities for computer-related abuses in the years ahead.\textsuperscript{18}

Although everyone seems to believe that the incidence of computer crimes has increased and is likely to increase still further in the future, it is impossible to get a precise measurement of just how many computer crimes have been committed. Believing that the crimes which have become generally known are only the "tip of the iceberg," those who are concerned about this phenomenon have come to fear that what has not been detected or reported may include not only far more crimes, but also the crimes of the greatest consequences.

The lack of knowledge of the incidence of computer crimes is, in many ways, no different than what has been historically true of all crimes, particularly the less violent or white-collar crimes. The incidence of computer crimes is believed to be greater than the numbers and losses reported, not only because of the inertia and reluctance to report crimes generally, but also because of a number of factors of special significance to this phenomenon. First, there is no consensus as to what should be classified as a computer crime. Much awaits the application of the precise definitions included in emerging federal and state computer crime laws.

Second, many computer crimes, though discovered, are believed to go unreported because of (1) a real or imagined fear of loss of public confidence, (2) the difficulty of proving that a crime has been committed, and therefore the risk of a false-arrest charge, (3) a concern about possible liability for the lack of prevention and recovery of losses, and (4) a belief by the computer user (and sometimes by the computer manufacturer) that public exposure would be tantamount to an admission that the computer is vulnerable to still further penetrations, as well as instruction as to how to effect such penetrations.

Third, computer crimes are more often than not difficult to detect. Computer frauds lack visibility: changes in a computer program can be removed after the offense has taken place, or the change may affect only a minuscule portion of the processed data, or the fraudulent manipulation may be programmed to take place at a predetermined future time. Indeed, in the vast majority of cases, detection has been a matter of sheer accident, rather than as a result of an ongoing security or auditing effort.

In spite of these difficulties, estimates of the level of computer

\textsuperscript{18} Id. at 27 (statement of John C. Kenney, Deputy Ass't Atty. Gen., Crim. Div., Dep't of Justice).
crime have been made. A well-regarded study, which began in 1971, involved searching out and analyzing computer crimes. It provides a better understanding of both the nature of these crimes and those who have perpetrated them. The study also provides a fairly reliable measure of the reported incidences of computer crime. By 1978, some 580 cases had been analyzed, with seventy-five percent of them verified by the investigators. The losses resulting from these cases totaled $280 million, not counting the $2 billion loss from the Equity Funding fraud.

Beyond the boundaries imposed by the limited detection and reporting of computer crimes, the full reach of their incidence has also been obscured by the handicaps facing relatively uninformed prosecutors, judges and juries in dealing with the complexities of computer technology under existing case and legislated law. The rules of evidence have been strained in dealing with invisible, electronic impulses and copies of information where the original never disappears or shows any sign of having been copied. In speaking of the need for adapting criminal laws to meet these and other challenges in dealing with computer crimes, one noted authority has concluded that "should our system of laws fail to meet his threat, [the computer criminal] may, in fact, ring the death knell of our entire system of justice. The stakes are high indeed."

As computer technology evolves further, new opportunities for crime will be created and, it is feared, these crimes will entail larger and larger sums. Some existing avenues for crime will be precluded; computer crimes will increasingly displace other kinds of white-collar crime. While it is acknowledged that computer crimes will continue to rank below the incidence of errors and omissions and natural disasters as the most numerous causes of computer problems, these more predominant causes are better understood and generally better controlled than is computer crime. Computer crime, in contrast, is not well understood; neither the potential for loss nor the degree of vulnerability is known to many users, and sufficient cost-benefit methods of deterrence, prevention, detection, and recovery do not currently exist.

20. Hearings, supra note 17, at 56 (statement of Donn B. Parker, SRI International).
21. Id. at 57.
B. Technological Lag in Computer Security

The rapidly changing technology of computers has been accompanied by a lag in adequate safeguards. The complexity and usefulness of today's computer systems are not paralleled by a similar capacity to adequately control their use. Presently available computers cannot be said to be technically secure from the highly skilled malefactor. While significant advances in system security and auditability are being developed, they will not be available for some time. Most authorities estimate that fully secured computers are still eight to ten years away.24

Although built-in security has generally not been a design priority, computer manufacturers are now making significant efforts to build better security features into their designs, sometimes beyond what their customers are willing to use or pay for. However, even the highly touted transfer of programs into secret codes25 has limitations. There could also be theft and ransoming of the disk on which the encryption resides, or a criminal's encryption of otherwise readable data and then the ransoming of the encryption key to that data. A persisting problem in the development of more technically secure computers appears to be the inability to design hardware and general-purpose programs that will produce proof of the correctness of processed data.

To some degree, the technological lag in the security of computers is a result of the original premise of their design and manufacturing, i.e., that they were to be used in a benign, non-hostile environment. The aim was to provide maximum efficiency and convenience of operation by friendly, honest employees within secure locations to which fully-controlled, physical access was required. The advent of remote access and multi-access systems shattered what little validity this premise had. Not only have computers proliferated so that the realities of significantly more and more users must be confronted, but the programs which control access to computers are themselves now exposed to tampering. The opportunity for committing the entire range of computer crimes has surely grown.

C. Modernizing Crime or Committing New Crimes?

A deeper understanding of the nature of computer crimes can result from seeing them in relation to those earlier forms of illegal activities known as "white-collar crimes." Some commentators have

24. Hearings, supra note 17, at 59 (statement of Donn B. Parker).
25. Id. at 79 (statement of Robert P. Abbott, Pres. of EDP Audit Controls, Inc.).
concluded that computer crimes are entirely new,\textsuperscript{26} while others see them as the same old crimes in an up-to-date form.\textsuperscript{27} The preponderance of opinion,\textsuperscript{28} however, supports the view that the computer has changed both the form and the means by which the traditional crimes of fraud, theft, larceny, embezzlement, sabotage, extortion, and conspiracy are perpetrated, as well as created the opportunity for a new array of criminal conduct. In other words, computers and computer data are vulnerable to all of the crimes which beset manual recordkeeping and its information, and are also exposed to a new array of unique criminal activity.

In some instances, computer crimes entail applications beyond the traditional white-collar category. Today, someone can commit murder by computer simply by disconnecting a computer on which another's life-support system depends. A person can extract funds by gaining control over and then ransoming a computer facility. More likely to be viewed as representing different and new crimes, however, are those which exploit the computer's total displacement of human intervention in decision-making and processing of large quantities of repetitive transactions.

Called "automated decision-making applications," these activities were the subject of a special report by the Comptroller General of the United States.\textsuperscript{29} Although this report treated only the problems of computer errors caused by such things as inadequate communications in software development, and overly complex data-input forms, it is not unreasonable to speculate about the exposure of these "automated decisions" to criminal penetration of the programs that control the decisions and their supportive processing. For the federal government, it was projected that some 1.7 billion payments and other actions were processed by computers without anyone reviewing or evaluating their correctness. These transactions were composed of the following:

- unreviewed authorizations for payments or checks (excluding payroll) of $26 billion;
- unreviewed billings totalling $10 billion; and
- unreviewed requisitions, shipping orders, repair schedules, and disposal orders for material valued at $8 billion.\textsuperscript{30}

As one writer put it, "the computer accepts what it is given . . . . Human tolerance is not so accurate, maybe, but it is far more suspi-

\textsuperscript{26} See, e.g., G. McKnight, Computer Crime (1973).
\textsuperscript{27} See, e.g., A. Bequaï, supra note 22, at 2.
\textsuperscript{29} Comptroller Gen., Improvements Needed in Managing Automated Decisionmaking by Computer Throughout the Federal Government (1976).
\textsuperscript{30} Id. at 9.
The entire thrust of current efforts to deal with computer crime through more focused study, security, and special legislation and prosecution seems to represent an attempt to view those criminal actions which affect a computer and its data in a new light. The attack upon computer crime—because of both the awesome potential of its incidence and the growing dependency of all citizens upon computers—merits consideration as a new phenomenon, one in which different kinds of perpetrators, new and more complex environments, new methods and urgencies, new jargon (such as "superzapping," "Trojan horses," "salami techniques," and "piggybacking"), and new forms of property are involved. To do less than focus specifically upon computer crimes apart from other criminal acts will not sufficiently arouse the general public, the makers and users of computers, or government leaders, to the risks of computer crime and awake them from their false sense of security.

D. Kinds of Computer Crime

There is yet no general agreement upon what constitutes a computer crime. Some authorities emphasize the use of the computer to steal large sums of money; others include the theft of services; and still others define the term more broadly to include the perpetration of any scheme to defraud others, as long as the computer is used to commit the crime. One authority emphasizes the computer—as either the tool or the target of the criminal—as the only essential commonality. Under this definition a computer crime occurs when (1) the computer is used to commit a crime of deceit, concealment or guile for the purposes of obtaining property or advantage; or (2) an action is taken to threaten or force action against the computer itself or its programs or other data.

The potential loss from computer crimes is considerable. Fraudulent manipulations of large aggregations of data are no longer tedious. These acts need neither be visible nor involve accomplices. One analysis of 150 major cases of computer fraud reported that for corporations, accounting and inventory control fraud involved average losses of $1.3 million, while fraudulent payments to creditors averaged $324,000 and fraudulent payroll distributions averaged

31. G. McKnight, supra note 26, at 155.
32. Hearings, supra note 17, at 155.
33. Id.
34. Id.
35. Id.
36. A. Bequai, supra note 22, at 4.
37. Id.
$139,000.38 This same study reported that prior to 1977, major computer crimes occurring in state or local government units averaged $329,000, and the average for federal agencies was $45,000.39

The variety of crimes committed with or to a computer is also extensive. Of fifty computer crime investigations conducted in 1978 by the Federal Bureau of Investigation, almost forty involved the alteration of a computer's input, e.g., the coded deposit tickets of a bank, the codes used for materials listed on purchase invoices.40 The remaining cases involved the use of a computer to keep track of kickbacks, the theft of computer programs, and the alteration of programs.41 Donn Parker has projected that future computer crimes will include massive frauds, extortion through gaining control over or causing destruction of computers directly affecting human life, terrorism, tapping of communication circuits, and hoaxes using computer output.42

In its major study of computer-related crimes in federal agencies, the General Accounting Office defined computer-related crimes to be “acts of intentionally caused losses to the Government or personal gains to individual related to the design, use or operations of the system in which they are committed.”43 Though having to rely upon reports of the direct investigative agencies, GAO learned of sixty-nine such crimes involving losses of $2 million.44 The majority of cases—about sixty-two percent—involved wholly or partially the preparation of fraudulent input.45 The remaining cases consisted of the unauthorized or inappropriate use of computer facilities and supplies (26%), the unauthorized processing or altering of information or its destruction (23%), and misappropriation of computer output (17%).46 The GAO characterized most of the crimes studied as relatively unsophisticated, requiring only limited technical knowledge from their perpetrators.47

The nature of computer crime can be summarized in terms of

39. Id. at 54.
41. Id.
42. Id. at 59 (statement of Donn B. Parker).
43. GEN. ACCOUNTING OFF., COMPUTER-RELATED CRIMES IN FEDERAL PROGRAMS 3 (1976) [hereinafter cited as GAO REPORT]. See also Taber, supra note 19, for a criticism of some of the findings of this study.
45. Id. at 5.
46. Id. at 6.
47. Id. at 5.
the variety of offenses that can be perpetrated upon a variety of property having a computer as an essential part of their existence. The matrix of property/offense relationships in Figure 1 leads to the identification of fifteen different kinds of computer crimes.

NATURE OF COMPUTER CRIME

<table>
<thead>
<tr>
<th>Offense Against Property</th>
<th>Kinds of Property</th>
<th>Hardware/Systems</th>
<th>Supplies</th>
<th>Services</th>
<th>Programs/Software</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer as Target</td>
<td>Physical Damage</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
</tr>
<tr>
<td>Computer as Target and/or Tool</td>
<td>Theft</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
</tr>
<tr>
<td>Computer as Tool</td>
<td>Unauthorized Alteration</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td></td>
</tr>
<tr>
<td>Computer as Tool</td>
<td>Unauthorized Use</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td></td>
</tr>
</tbody>
</table>

FIGURE 1

III. COMPUTERS AND CRIMINALS

Computers are used and misused by people. Commiting a computer crime is a personal act. Without individuals who view computers and their data as opportunities for unearned reward, there would be no computer crime. No matter how complex or ingenious a particular computer or a specific computer crime may appear, the principal focus must remain on those who would commit such an act. Surely, the most vulnerable element in the use of computers will remain the human element.

A. General Profile of the Computer Criminal

While some authorities speak of the "computer criminal" in a manner which implies a uniformity of personal characteristics and background, most contend that there is only a broad outline which
serves principally to distinguish the users of computers in crime from more traditional criminals.48 Those who perpetrate crimes with or to a computer tend to be young—eighteen to thirty years old—though this range is likely to widen. They have high aspirations, are aggressive, highly intelligent and personable. They are technically competent in electronics or have some computer skill. Often among the most attractive job applicants, they tend to be inadequately challenged in their jobs.

Perpetrators tend to be amateurs, rather than experienced criminals. The vast proportion of those known to have committed computer crimes were employees of the organization having the computer. They performed their unauthorized acts within their own work environments using their own specialized capabilities and, oftentimes, taking advantage of their positions of trust. Many have acted in collusion, though the likelihood of collusion diminishes as one moves up the corporate hierarchy. It is not clear whether this inferred high incidence of collusion in computer crimes is a function of the need for a combination of resources, or a result of the fact that computer crimes involving more than one person are more frequently detected.

B. Segments Within the Known Perpetrators

Beyond this general profile of the computer criminal, other observations can be made which provide further insight into the human dimension of this problem. It is important to remember that there is a general belief that numerous computer crimes go undetected. Therefore, it is not known whether this or any other discussion of the computer criminal based upon those who are apprehended is representative of all persons who have committed such crimes. Indeed, some contend that the most clever and, therefore, the ones to be most concerned about are those who have never been caught or, if caught, have never been publicly exposed.

Perpetrators of computer-related crimes are those people who have access to computer input, output, or stored data, or the customers who can take advantage of the manipulated data. In the minds of some, the computer criminal appears as a most sophisticated criminal, very much able and intent upon outwitting the most technically advanced computers, their physical security, and their control systems. Others picture the computer criminal as someone who takes advantage of a weakness he only accidentally discovers in a computer’s design or programming. There are also those who are

48. See, e.g., A. Bequai, supra note 22, at 3-5; Hearings, supra note 17, at 58, 59 (statement of Donn B. Parker).
worried about persons with no special knowledge of computers, but who might seek to damage a computer and its data in an act of vandalism or sabotage.

The apprehended computer criminal has tended to be a first timer, perpetrating his one big, criminal act. Oftentimes, the act is a spontaneous response to (1) an emotional difficulty besetting the perpetrator and (2) a perceived opportunity to exploit a computer to help in resolving that difficulty. An individual's integrity is surely tested at such a time, particularly when he believes that the likelihood of detection is limited and, even if apprehended, the possibility of successful prosecution is small. As computers come to be more and more widely used, the perpetration of a computer crime will more likely be seen as a "way out" during times of stress.

Although the Department of Justice has indicated that it has no evidence that "organized crime" has systematically moved into the field of computer crime, some authorities are fearful about its future involvement. The mere fact that increasingly large sums are being stored in computers, and that they are exposed to relatively undetectable thefts, leads some to predict greater interest and involvement by career criminals. Certainly, the capability to commit these crimes is readily available to them. Amassing the specialized talents, such as those of programmers, accountants, wiretappers and burglars, would also not be new to them.

C. Motivational Influences Leading to Computer Crime

Given this backdrop of those who have committed computer crimes in the past, it is also useful to look at why they have perpetrated these acts. As previously indicated, the motivation is commonly a specific thing that, while possibly active for some time, has more to do with the situation and personal beliefs than with any firm, criminal tendencies.

Some specific motivations which have been identified in extensive interviewing of persons committing computer crimes and careful review of their and other cases include:

- to secure personal reward or power;
- to engage in a challenge, beat the system, game playing;
- to play "Robin Hood," that is, get back at the government, telephone company or other large impersonal corporation;
- to "take on" the emotionless machine;

49. Id. at 112 (statement of John C. Kenney, Deputy Ass't Atty. Gen., Crim. Div., Dept't of Justice).
50. D. PARKER, supra note 23, ch. 7.
• to exploit an opportunity and give a "lesson" to someone who failed to take sufficient precautions;
• to vent specific or general resentment against one's employer, supplier, banker or government;
• to act out in a mischievous manner; and
• to "take on" a major visible representation of modern technology, one that also is a principal means of the concentration of economic power.

In considering these motivations, one needs to remember that many persons in the electronic data processing field currently give effect to these motivations in what are commonly accepted today as playful, "innocent" incidents. Such "harmless" activities as making a Snoopy calendar or entering one's bowling scores into the computer can obscure what is correct, proper and legal. At the same time, these acts can, and have, spilled over into uses which provide a source of remuneration for the unauthorized user. They have also been a ready excuse for what is more surely a criminal act. In light of the finding that the computer of one federal agency (Department of Agriculture) was accessed for unauthorized purposes by employees more than 6,400 times in one twelve month period (seventeen times a day), it is essential that computer users more specifically label the purposes believed to be criminal.

IV. DEALING WITH THE PROBLEM OF COMPUTER CRIME

Though a truly penetration-proof, computer operating system is highly unlikely, much more can be done to deter, discover and punish those who commit computer crimes. To some extent, the present technology of computer security is a limiting factor. At the same time, many of the available security measures have not been applied by computer users—sometimes because of their cost, but often because of a lack of concern. There are, moreover, serious limitations upon the effective reporting, prosecution and punishment of those who are apprehended. For significant improvements to be realized in both the deterrent/detection and the punitive approaches to the problem of computer crime, legislation which effectively updates case and statutory law is necessary.

A. Crime Deterrence Through Improved Computer Security

The members of the American Society for Industrial Security ("ASIS") recommend a number of specific guidelines for improved

They believe that the best preventive measure is a "good defense." With the risk of computer crime growing, these security experts are concerned about users who continue to view computer security in too inconsequential a role. Although they recognize that the defense for each computer facility must be designed with such considerations as type of access, system and principal applications in mind, they contend that all computer users should build the following security elements into their operations:

- "separation of knowledge" through division of responsibilities, job rotation, physical isolation, controlled access, logging of stoppages and interruptions;
- written programming instructions with threat monitoring and audit trails built in;
- careful accounting of all input documents;
- periodic changes in access codes and passwords; and
- scramblers and cryptographic applications in data transmission.\(^3\)

Such security provisions as these identified by ASIS are believed to have reduced the threat from many individuals who have the opportunity to commit computer crimes. There is, however, an increased opportunity for criminal acts by those upon whom the installed security measures depend and in whom increasing levels of trust must be placed, simply because of the sophistication of emerging technology. Since a compensating kind of security cannot yet be designed into the computers themselves, there must be operational, procedural, managerial and personnel security precautions which go beyond those of mere physical control.

Top management must see the need for a multi-faceted program of continuing vigilance and accountability. Every one of the sixty-nine cases of computer crime reviewed by the General Accounting Office in 1976 was directly traceable to weakness in system controls, believed by the GAO to be a result of management failure to recognize the importance of controlling computer systems.\(^4\) Internal controls must be both designed and enforced. Similarly, computer control processing programs must be designed to be auditable and a highly visible and active program of computer auditing must be implemented.

IBM has developed specific recommendations for improved security, to some extent as a result of a concentrated $40 million effort to realize greater security in the design and use of its own com-

\(^{52}\) Hearings, supra note 17, at 115 (statement of the Am. Soc'y for Indus. Security).

\(^{53}\) Id. at 115, 116.

\(^{54}\) GAO REPORT, supra note 43, at 9.
computers. It urges that action be taken by computer users in four areas: (1) rigid physical security; (2) new identification procedures for input operators; (3) new internal auditing procedures based upon retaining a fuller record of each computer transaction; and (4) new cryptographic symbols to scramble information. Still, this manufacturer's director of data security has observed, "[t]he data security job will never be done—after all, there will never be a bank that absolutely can't be robbed." Following his analysis of 150 computer fraud cases, one authority concluded that most computer crimes could be prevented by a "tight system of internal control." He recommended (1) stricter controls of input transactions; (2) rigorous audits; (3) improved management supervision based upon responsibility reporting; (4) program controls including independent verification and better physical security; (5) control of data files; and (6) a more disciplined operation of the entire data processing function.

In general then, the need is for assuring that computer facilities, their telecommunications networks, and data bases are protected from intentional loss, damage or unauthorized use. Through a comprehensive program of carefully devised policy directives, administrative procedures and control mechanisms, and technical capabilities designed into both computers and computer programs, much can be realized. Many of these efforts will result in greater overall system integrity—simultaneously leading to greater physical and access security from criminal acts, accidental harm, and invasions of privacy having no criminal intent. Just as important, they will provide a greater capacity for early discovery of wrongdoings and more reliable evidence should a crime be detected.

There is, of course, an economic dimension to the consideration of the best means of greater computer security. Even when they recognize the need and are fearful of the immediate risks they face, most users require that the particular measures proposed for implementation be "cost justified." Special care needs to be taken, however, to ensure that such a requirement does not preclude a reasonable consideration of all of the possible hazards and risks of computer crime.

The focus should be on taking security actions which are reasonable in their cost to reduce the probability of a loss to an accept-

---

55. Leepson, supra note 1, at 13.
57. Allen, supra note 38, at 52.
58. Id. at 52, 53.
ably low level. The true extent of all possible losses to asset values as well as the probable obstructions to accomplishing one's mission which can result from computer crimes must be fully weighed before preventive action is taken. No organization can afford to wait for the occurrence of a major loss to provide quantification for the economics of their computer security.

As more and more senior managers become concerned with possible losses and the technology of computer security catches up with the technology of computers, a true protective net will be spread over computers and data. An overall security program having diverse elements, but designed and implemented in a coherent fashion, would consist of all of the following classes of protection for the computer hardware, programs and data involved:

- positive, unique identification of people, devices and other specific resources;
- authorization of all critical system integrations between people, data, programs, devices and other specifiable resources;
- surveillance of system activities with strict personal accountability identified for each; and
- system integrity, including not only physical security but also protection against wiretapping and eavesdropping.

Such a program will not only make it demonstrably difficult for the perpetration of a crime through unauthorized access, but will also make far more difficult the misuse of an authorized access capability. Beyond increasingly controlled physical and remote access, much more in the future can be expected from encryption of programs and the freezing of programs into what is known as "firmware." In both of these approaches, however, the technology is not yet complete and is very costly to apply. More critically, these and other new security approaches tend to be "passive," that is, they neither detect an attempt to commit a criminal act, nor report it.

It is no overstatement that computer security measures will continue to fall far short of what is possible, let alone what is needed. In computer facility after computer facility there must be a serious effort made to confront the problem of computer crime and to take whatever measures are reasonably possible to achieve a more manageable, predictable, reliable and non-penetrable system. The need for such a system outweighs any unavoidable, negative impact which might come from performance degradation and human inconvenience.

B. Punishing the Computer Criminal

The principal restraint upon those who have considered the per-
petration of a crime has been the possibility of having to face negative consequences: discovery which comes to the attention of peers and others whom they regard highly, publicized prosecution, and punishment. For many, the distaste of these consequences are sufficient, particularly so if the stigma, fine and/or imprisonment is more significant than the possible rewards. Since no computer user can be assured that even the best conceived and executed security measures will remove the risk of crime, apprehension and effective punishment remain a critical means of confronting the problem of computer crime.

Most authorities, however, do not believe that the fear of punishment is currently a strong deterrent. Under existing laws, reporting is still shunned; prosecution remains complex, uncertain and costly; and sentencing too illusory for the fear of punishment to be a serious obstacle. There just does not seem to be much evidence that the negative consequences are that great when compared with the ever-growing rewards. Indeed, stories of denials of losses, perpetrators who are rewarded to assure their silence or to refrain from a false arrest charge, and minimum or unsupervised suspended sentences continue to appear.

Some computer criminals have received notoriety for their creativeness. Some even become consultants in the prevention of computer crimes by others. One current computer security consultant was reported to have previously stolen over $800,000 worth of equipment from a large telephone company. He pleaded guilty to one count of grand theft of $5,000 worth of equipment and was sentenced to two months in a minimum security correctional institution. He served fifty days and paid a $500 fine.59

One authority spoke of the impending danger resulting from the major discrepancy in the sentencing of computer criminals, when he observed,

In early August 1977 a deaf-mute was sentenced, by an Ohio court to 1 to 10 years in prison for stealing a bottle of beer. Several months before, a Maryland court sentenced a computer felon to three years probation. The latter had been involved in a fraud that exceeded $100,000. Computer felons are a serious threat, not only to society, but also to the confidence of the public in our system of justice. [Such a] legal system . . . invites disrespect and scorn. It invites felons to change their techniques, rather than their ways.60

Strong penalties and a judicial resolve to mete them out can produce the desired deterrent effect only if the victims report the crimes and the investigators and prosecutors are sufficiently in-

60. A. BEQUAI, supra note 22, at 196-97.
formed to act effectively. Fortunately, at the federal level, the Department of Justice has undertaken a concerted effort to provide all federal prosecutors and investigators (and some at the state and local level) with a general familiarity with computer technology and to add to its existing central cadre of attorneys and investigators having particular expertise in computer technology. Should a federal computer crime bill be enacted, it is expected that this effort will be intensified and more state and local investigators and prosecutors will be invited to participate.

C. Role of Computer Crime Legislation

At both the federal level and in some of the states, legislation has been enacted or is pending which focus the criminal laws on the realities of changing computer technology. Existing laws can, of course, still be used to provide avenues for prosecution in addition to the more direct legislation. The aim at the federal level and in those states where there has been legislative action on computer crime bills is to secure an all-encompassing act. These bills and laws make it no longer necessary for prosecutors to "shoe horn" their cases into statutes and case law, which neither considered the technical complexities of computers, nor the kinds of criminal acts which involve computers. The severe procedural and evidentiary handicaps which have so often accompanied the use of existing laws are not obstacles under these bills and acts. Senator Abraham Ribicoff (D-Conn.) has spoken of his sponsorship of the proposed federal bill as helping to close "a big hole in the criminal justice laws of our country."

Throughout the hearings, discussions and negotiations that have taken place on computer crime legislation, a number of objectives of these bills have been emphasized:

- to facilitate the preparation of evidence and prosecution of computer crimes;
- to remove the gaps and inconsistencies in existing laws and cases so as to simplify judicial responses;
- to improve the likelihood of more appropriate punishment; and

---

61. *Hearings, supra* note 17, at 44 (statement of Joseph E. Henehan, Chief, White Collar Crime Sec., Fed. Bur. of Investigation); id. at 45 (statement of Mark Richard, Chief, Fraud Sec., Dep't of Justice).
62. See the Appendix in the next issue of the Journal.
They have been very little, if any, attempt to claim more for this specialized legislation than that which is indicated by these objectives. Specialized legislation will not eliminate computer crime. The proponents do not overlook the continuing need for improved computer security, technological improvements in the security dimension of computer design, effective investigations and prosecutions, and a greater regard for ethical standards among those employed in electronic data processing jobs. All of these are needed; no one is sufficient by itself.

Strong legislation which specifically focuses upon computer crime can be salutary to the entire range of possible preventive and punitive actions. Foremost, it can reassure the many individuals employed in using computers or who otherwise come into contact with computers that it is worthwhile for them to obey the law. They will know that their efforts will more surely be perceived by others as lawful and that those who engage in unlawful practices will not be as likely to benefit at their expense. Effective legislation will also encourage those who discover computer crimes to report and to cooperate in the prosecution of the perpetrators.

As the successful applications of such a law mount, the voices of those who advocate greater investments in computer security and aggressive prosecution will be reinforced. They will not only be able to provide demonstrable proof in terms of specific risks, but will also feel less awkward or embarrassed, since they will be aiding in the prosecution of conduct about which many are noticeably aroused. Successful prosecutions under a specific computer crime bill will increasingly exert a force for preventive action. All users, particularly those using the computer to fulfill a fiduciary responsibility, can be expected to strive to prevent those acts enumerated in the law, report the acts that do occur, cooperate in the gathering of evidence, and support a request for the maximum possible sentence and fine.

As time goes on, computer manufacturers will find it more and more realistic to reorder the priorities they have assigned to security in the design of their computers. They will not want to risk being sued as an accessory to crime or for malpractice for the programs they provide. Neither will they want to risk the possibility that such legislation might bring them to a point where they have to defer a new application or a new design because they are unable to reassure users that there will be no outbreak of crime from its introduction.

Computer crime legislation will have several beneficial effects for prosecutors and judges. There will be less uncertainty as to the
charges that should be made, thereby making it easier to assemble the evidence and to expedite prosecution. There will also be less need for the courts to make esoteric, academic findings in their endeavor to link unauthorized use of computer technology to general criminal legislation that never contemplated the existence of computers.

V. ALTERNATIVES FOR LEGISLATIVE ACTION

The need for legislation which specifically deals with the threat of computer crime is widely recognized today. The general vulnerability of computer users, the uncertain applicability of existing common and statutory law, and the very complexity of the possible criminal acts all have led to pressures at both the federal and state levels to enact computer crime legislation.

At the federal level, considerable support has developed on behalf of the Federal Computer Systems Protection Act (S. 240). Eleven states have already passed laws, and several others are known to be considering laws aimed at both deterring would-be computer criminals and easing the task of securing appropriate punishment of those who do commit crimes involving a computer and its data.

These laws do not deal with the problem in a uniform way. Rather, their diversity suggests that there may be no one best approach, and that they are only alternatives about which any lasting conclusions must await prosecutorial and judicial experiences. New critical issues may arise and gaps may be discovered as computer technology continues to change.

A. Prosecution Under Existing Laws

Prior to the enactment of the Florida law in May 1978, what criminal actions were brought against those using computers for unlawful advantage were brought under common or case law or one of the sections of various federal and state laws into which they could reasonably "shoe-horn" the alleged acts. At the state level, reliance was on the laws dealing with (1) crimes involving habitation and occupancy or (2) offenses involving property.

Among the more general habitation offenses which have served

65. As of June 1980, the following states had enacted computer crime legislation: Arizona, Virginia and Florida in 1978, and California, Colorado, Illinois, Michigan, New Mexico, North Carolina, Rhode Island and Utah in 1979. For the texts of the enacted legislation, see the Appendix in the next issue of the Journal.

66. For the texts of these bills, see the Appendix in the next issue of the Journal.

as the basis for prosecution of computer crimes at the state level are arson (burning with malice) and burglary (felonious intent to commit larceny or, more recently, any crime). About a dozen property-theft crimes have been applied in one form or another to computer criminals. They include such offenses as taking property in the possession of another for purposes of larceny, embezzlement (a statutory crime), false pretenses (also statutory), extortion, malicious mischief, forgery, and receipt of stolen property.

In seeking to prosecute a theft of or damage to a computer program on the basis of the law dealing with property, the presence of a crime often turns on whether the program will be found to be within the meaning of the term “property” as used in the law. The common law test of tangibility in determining what constitutes personal property is not readily seen to include computer programs. Similarly, some cases, in New York for example, have held that only tangible or physical property can be damaged, thereby effectively excluding the prosecution of malicious alteration or destruction of programs.

At the federal level, Title 18 of the United States Code contains forty statutes which might be used to prosecute computer-related crimes, depending upon the specific circumstances of a case. The key legal authority for federal prosecutors has derived from the mail fraud statute and, to a lesser extent, the wire fraud act. In some instances, consideration has been given to amendments which could resolve existing ambiguities, such as those which exclude electromagnetic impulses from being considered under the wire fraud statute.

68. A. Bequaï, supra note 22, at 25.
69. Id. at 26.
70. Id. at 29-31.
71. Id. at 31.
72. Id. at 31-33.
73. Id. at 33.
74. Id. at 33-34.
75. Id. at 34.
76. Id. at 34-35.
77. Hearings, supra note 17, at 70 (statement of Susan H. Nycum, Chickering & Gregory, San Francisco, and investigator with Donn Parker in the computer abuse study).
78. Id.
79. Id.
80. Id. at 6 (statement of Sen. Abraham Ribicoff).
81. A. Bequaï, supra note 22, at 37-38.
82. Id. at 38-39.
Also of some assistance in the prosecution of computer crimes at the federal level have been the embezzlement and theft statute covering federal agencies; the banking statutes; and the law dealing with false entries in the records, reports, and transactions of banks and federal credit institutions. Other laws possibly relevant are those which protect federal property from malicious destruction, punish arson, and deal with conspiracy to defraud the federal government. Also applicable might be the federal bank robbery and disclosure statutes. In the case of federal agencies, thefts of computer programs, as well as their destruction or damage, have been successfully prosecuted under existing federal statutes dealing with property.

Some of the success at the federal level has come about because of the very uneven and limited capabilities of state authorities. In at least one case, federal prosecutors were fortunate to discover that the defendant had made two of his forty telephone calls to access (without authority) his former employer's computers in Maryland from his Virginia office, thereby engaging in an interstate activity, without which there would have been no federal jurisdiction.

There are instances where statutes and case law which do not deal with criminal acts have been specifically modified to take account of computer technology. In both North Carolina and Delaware, there are laws which directly address computerized records, recognizing them as having unique properties and capable of being converted into written form within a reasonable period of time. In Florida, the business records statute has been amended to include records "kept by means of electronic data processing." In 1972, Illinois courts dealt with the first criminal case involving computer output. In People v. Gauer, the accuracy and reliability of a telephone company's computerized records of telephone calls became an issue in a case remanded for a new trial. Common-law doc-

83. Id. at 39-40.
84. Id. at 40.
85. Id. at 40-41.
86. Id. at 41.
87. Id.
88. Id.
89. Id. at 42.
90. Id.
91. Hearings, supra note 70, at 71 (statement of Susan H. Nycum).
93. A. Bequai, supra note 22, at 128-29.
94. Id. at 129.
95. 7 Ill. App. 3d 512, 288 N.E.2d 24, 4 CLSR 477 (1972).
trine has also been expanded at the federal level to meet the needs of computerized recordkeeping by passage of the Federal Rules of Evidence Act.\textsuperscript{96}

\textbf{B. Federal Computer Systems Protection Act}

In January 1979, a law first introduced in June 1977 and described by one of its principal sponsors—Senator Abraham Ribicoff (D-Conn.)—as making “virtually all unauthorized use of federal computers and computers used in interstate commerce a federal offense,”\textsuperscript{97} was reintroduced. A number of revisions suggested by the Department of Justice and computer security experts were made in the January 1979 revision. The major change provided for stiffer fines of as much as two and one-half times the amount of the fraud or theft (as contrasted with a maximum of $50,000 in the original proposal).

Senator Charles H. Percy (R-Ill.) was the other principal sponsor of this proposed legislation. Under the Federal Computer Systems Protection Act of 1979,\textsuperscript{98}

(a) Whoever knowingly and willfully, directly or indirectly accesses, causes to be accessed or attempts to access any computer, computer system, computer network, or any part thereof . . . for the purpose of (1) devising or executing any scheme or artifice to defraud or (2) obtaining money, property, or services, for themselves or another, by means of a false or fraudulent pretenses, representations or promises . . . .

(b) Whoever intentionally and without authorization, directly or indirectly accesses, alters, damages, destroys, or attempts to damage or destroy any computer, computer system, or computer network . . . , or any computer software, program or data contained in such computer, computer system or computer network . . . .

can be found to have committed a computer crime.

As the first federal law prepared specifically to control crime by computer and unlawful damage to computers, this act sets forth a new, comprehensive section to be added to chapter 47 of Title 18, United States Code. In addition to computers owned or operated by the United States, this law specifically refers to the computer systems of financial institutions (specifically those insured by the Fed-


\textsuperscript{97} Hearings, supra note 17, at 7 (statement of Sen. Abraham Ribicoff).

COMPUTER CRIME

eral Deposit Insurance Corporation, the Federal Savings and Loan Insurance Corporation, the National Credit Union Administration, and the Securities Investor Protection Corporation, members of the Federal Reserve, home loan banks, and broker-dealers registered with the Securities Exchange Commission).\textsuperscript{99}

The law is designed to aid federal prosecutors in confronting the "four main categories of computer crime":\textsuperscript{100}

- introduction of fraudulent records or data into a computer system;
- unauthorized use of computer-related facilities;
- alteration or destruction on computerized information or files; and
- theft by electronic or other means of money, "financial instruments" such as checks and credit cards and "valuable data" such as computer programs in machine or human readable form.

This federal legislation is viewed as a beginning effort to address the problem of computer crime, making the perpetrator of such criminal acts clearly punishable by sizeable sentences and fines. It would remove the requirement that telephones or other forms of illicit computer penetration take place across a state line in order to justify federal prosecution. It would ease the present jurisdictional and evidentiary burdens upon law enforcement and prosecutorial personnel. Its specificity and the unprecedented large fines which it authorizes are expected to do much to deter the potential computer criminal, in "an important signal to the world of white collar crime that the Federal Government will commit itself to deterring this type of criminal activity."\textsuperscript{101}

The need for federal legislation appears to be principally a function of the complexity and geographical breadth of both computer activities and the criminal acts which involve them. Its passage is expected to justify the significant concentrations of experts necessary to deal with such crimes and minimize the dilutive effect from any conflicting and contradicting state acts. Federal action may also lead to legislative efforts in the various states, with the states following the federal "model" to some degree to deal with intrastate crime, as well as facilitate state-federal cooperation in broader investigations and prosecutions of computer criminals.

In testifying on behalf of computer crime legislation at the federal level before the Senate committee considering the Federal Computer Systems Protection Act, Susan H. Nycum (consultant to the National Science Foundation sponsored study of computer

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{99} S. 240, 96th Cong., 1st Sess. (1979) (as amended).
\item \textsuperscript{100} Hearings, supra note 17, at 7 (statement of Sen. Abraham Ribicoff).
\item \textsuperscript{101} Id. at 3 (statement of Sen. Joseph R. Biden, Jr.).
\end{itemize}
\end{footnotesize}
abuse) recommended changes to enhance the effectiveness of the federal bill. She emphasized five concerns:

- the bill can apply equally to the theft of a ten dollar pocket calculator as to the theft of a multi-thousand dollar minicomputer;
- disparities exist between the penalties of this act and those of existing laws which cover the same actions;
- definitions included in the bill are unduly restricted to current technology;
- certain categories of abuses are not treated or are inadequately or inconsistently treated in the bill; and
- the bill is premature in suggesting a role for licensing or formal certification of computer products and professionals.

Critical in some of the other testimony at the hearings was the suggestion that the provisions become effective only after a period of one to two years after being signed by the President. The ensuing period would allow for full dissemination and improvements in the users' administrative policies and controls over physical access as they seek better preventive security under stimulus of the law. Another significant issue can be raised about the revised version insofar as it proposes to calculate fines on the basis of the extent of the loss. As established in the present draft, the fine in cases of fraudulent use of the computer or theft is to be based upon a maximum of two and one-half times the amount of the fraud or theft, or $50,000, whichever is greater. Such a value is not always readily calculable and value is not always the only element of significance in computer crimes.

The proposed Federal Computer Systems Protection Act was meant to work in conjunction with [existing federal laws] to facilitate the task of federal prosecutors in the area of computer crime. [It] does one thing that other statutes do not: it addresses itself specifically to the problem of computer crime. [It was] made as broad as possible, to be effective against the many types of computer crime. [It is] a simple and yet effective statute... made sufficiently broad to include all "electronically produced data." New legislation is needed not to replace but rather to supplement the present arsenal.

102. Id. at 71-73 (statement of Susan H. Nycum).
103. Id. at 68, 69 (statement of Donn B. Parker); id. at 125, 126 (statement of Edward J. Palmer, Exec. Dir. of Data Processing Management Ass'n).
106. A. BEQUAI, supra note 22, at 45-46.
C. Emerging State Legislation

Eleven states have passed legislation specifically dealing with computer crime.\(^{107}\) The other states continue to depend either upon statutes which make no reference to the computer or entirely upon common law. Relevant legislation is known to have been introduced in several other states.\(^{108}\) In 1978, Rhode Island passed a law dealing with “fraudulent communication devices,” in which reference is made to use of an “electronic” device and “electronically” obtained communication service without authorization.\(^{109}\)

The purpose of these state computer crime laws has been to close the gaps in existing law insofar as computer technology can be used in ways which are neither clearly unlawful nor easily prosecuted, but are nevertheless harmful to users and those they serve. Describing the motivation behind the state’s law passed in 1978 with the active support of his office, the Attorney General of Arizona said that there was a “belief that Arizona theft (ARS § 13-1802) and fraud (ARS § 12-2310) statutes [did] not adequately deal with the problem of person or persons who are detected inputting, outputting or erasing data from a computer without authorization when the facts as determined do not sufficiently disclose the fraudulent scheme or the theft in tent.”\(^{110}\) The Arizona law criminalizes fraudulent conduct even if no misrepresentations are made.\(^{111}\)

The Arizona and Florida laws directly resolve the issue arising from the intangible and electronic-impulse nature of computerized information. Also confronted is the question of the value of such information, the processing time of a computer, and creative services in the form of software.

In drafting Arizona’s statute, the Federal Computer Systems Protection Act was used as a model.\(^{112}\) The Arizona law contains few differences other than the penalties authorized. The law includes statements of computer fraud in both the first and second degrees as well as definitions of such specific terms as “access,” “computer,” “computer program,” “property,” and “services” as used in these statements. These provisions were made part of the “Organized Crime and Fraud” Chapter of Arizona’s statutes.

\(^{107}\) See note 65 supra.

\(^{108}\) The texts of these bills will be reprinted in the Appendix in the next issue of the Journal.

\(^{109}\) R.I. GEN. LAWS §§ 11-52-1 et seq.


\(^{111}\) Id. at 143.

\(^{112}\) Id.
Florida's Computer Crimes Act\textsuperscript{113} is more of a stand-alone bill than Arizona's. While using some of the definitions of the federal law, it is more elaborate. It specifically includes "intellectual property," defining it as "data including programs." It also establishes different levels of possible penalty (misdemeanor or felony) on the basis of (1) whether the offense is against intellectual property, computer equipment or supplies, or against computer users; (2) whether the offense is one of damage and destruction or fraud; (3) the amount of the damage to the computer or supplies; and (4) whether or not the offense results in "interruption or impairment of governmental operation or public communication, transportation or supply of water, gas, or other public service."

Far less elaborate is the California law.\textsuperscript{114} While also a stand-alone statute, it modifies the existing Penal Code by inserting only two broad statements as to what constitutes computer crime. Similar to those in the federal bill, the California provisions outlaw (1) use of a computer to defraud or obtain money, property or services by means of false pretenses, representations or promises and (2) intentional use of or damage to a computer or its data. The maximum punishment in either type of crime is $50,000 or two, three or four years imprisonment, or both. A specific sum is appropriated for allocation and distribution to local agencies to reimburse them for costs incurred by them pursuant to the act.

VI. CONCLUSION

For those state legislatures which recognize the desirability of a computer crime law, consideration needs to be given to a number of elements that are critical to the effective application of such a law. These elements include:

- broad legislative concern with all forms of computer crime;
- integration of this concern into existing criminal law (both statutory and case law);
- limited scope in terms of dealing as specifically as possible with the more flagrant, less acceptable abuses of computer technology;
- definitions consistent with those of other computer crime legislation and emerging industry standards;
- significant, yet graded, penalties (fines and prison terms) in relation to the seriousness and value of the crime; and
- reasonable latitude for the exercise of discretion by the prosecutor.

To some extent, the critical nature of some of these considera-

\textsuperscript{113} FLA. STAT. ANN. §§ 815.01-815.07 (West Supp. 1979).
\textsuperscript{114} CAL. PENAL CODE § 502 (Supp. 1980).
tions is a function of the newness of the legislative approach to the problem. As experience with computer crime laws develops, there will be more certainty as to what constitutes "good" legislation and the significance of some of these elements may diminish.

While government can do little to minimize the public's dependence on computers, it can, and should, do whatever it can to minimize the public's dependence on computer criminals.