Chapter 5

Computer Crime

Contents

Tables

Chapter 5

Computer Crime

SUMMARY

This chapter focuses on evaluating the nature and scope of computer crime, and options to consider in designing effective computer crime legislation. Computer crime is defined here simply as a set of crimes in which computerized data or software play a major role. It is largely the intangible (but critically important) nature of computerized information that creates a need for special legislative attention to computer crime.

Since the 1970s, there has been a growing consensus that existing laws covering the variety of crimes that can be committed using a computer (e.g., fraud, theft, embezzlement, invasion of privacy, trespass) either do not cover some computer abuses, or are not strong and clear enough to discourage computer crimes and allow expeditious prosecution.

Some of this consensus is a result of publicity regarding "hackers" penetrating various computer systems. The hacker issue is frequently blown out of proportion, and although it cannot be ignored, crimes committed by dishonest or disgruntled employees who have authorized access to computers represent a far greater source of risk than outsiders penetrating information systems.

After a decade of examining computer crime, Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. The act provides a felony penalty for those who gain unauthorized access to computerized classified information, and a misdemeanor penalty for unauthorized access to the computerized information of financial institutions or the Federal Government. In addition, 45 States have passed computer crime laws.

OTA's major findings in this area are that:

- There is a scarcity of reliable information about the amount of computer crime occurring and the nature and severity of the crimes. The available evidence suggests that significant losses have occurred, though the full extent is unknown.
- Despite the lack of hard information, the vulnerabilities of organizations using computer systems are much greater than in the past, as discussed in chapter 4 on information systems security. Thus a consensus has emerged that a combination of Federal and State laws is appropriate in this area. Actions taken so far have set forth de facto Federal and State roles—namely, that while State laws will play a primary role in most cases, Federal legislation will concentrate on areas of special Federal concern.
- Legislation needs to balance concern about the potential urgency of the situation with other factors—in particular, the responsibilities of vendors, owners, and users for the security of their systems, and the need for keeping computer crime sanctions reasonably consistent with other criminal law and other aspects of U.S. information policy.

There has been substantial interest in further legislative action on computer crime in the 99th Congress. The legislative debate and hearings have identified the following actions that could clarify and/or strengthen the Federal role in monitoring, preventing, and prosecuting computer crime:

- extend the current Federal statute (Computer Fraud Act) to cover interstate crimes affecting private sector companies, while placing some limits on Federal jurisdiction;
- amend the conceptual approach to defining computer crime used in the Computer Fraud Act, for example, by focusing on the type of crime committed and/or the kinds of information unlawfully accessed;

- change or clarify the kinds of computerized information covered by the Computer Fraud Act, e.g., by restricting the portion of the act that outlaws unauthorized disclosure of information from Federal computers to apply only to Privacy Act information;
- extend or clarify the definitions of key terms used in the Computer Fraud Act, such as the definition of authorization;
- enact limited protection to computer crime victims in order to encourage prosecution;
- enact a penalty for computer crime convictions that would include forfeiture of equipment used;
- establish strengthened or new reporting systems for monitoring the nature and scope of computer crime; and
- establish a study commission to address computer crime (and perhaps related) issues.

INTRODUCTION

As noted in chapter 4, there are four major kinds of measures to protect information systems—technical, physical, administrative, and legislative. The first three were emphasized in chapter 4; this chapter will focus on the problem of designing and implementing Federal legislation that pertains to computer crime.

Generally, computer crime is a term used to refer to a loose set of frauds or abuses in which computerized data or software play a major role. The Department of Justice's *Criminal Justice Resource Manual* defines computer-related crime as "any illegal act for which knowledge of computer technology is essential for successful prosecution. "[1] Although some would include theft or physical vandalism of the computer itself in the category of computer crime, the focus of this chapter is on acts that involve manipulation (or theft) of the content of computers—data—for criminal purposes. It is largely the intangible (but critically important) nature of computerized information that makes computer crime a different kind of criminal act needing special legislative attention.

As table 5-1 notes, the computer can be used as a tool or instrument in a variety of activities that resemble distinctly different kinds of "conventional' crimes. While some computer crimes, for example, clearly look like embezzlement, others seem more akin to vandalism or the electronic equivalent of "joyriding." This wide variation in the nature of computer crimes is one of the factors that makes effective, comprehensive, and equitable legislation difficult to design.

Another aspect of computer crime that presents a challenge to effective legislation is the strong connections between this area of legislation and other social and administrative implications of information technology. For example:

- *Computer security* is clearly closely related, in the sense that computer crime laws are part of the arsenal of security measures, hopefully discouraging com-

Table 5-I.—Types of Computer Crime

End result of the crime	"Conventional" crime it resembles
Use of computers to embezzle funds or assets	Embezzlement
Destruction or alteration of software or data	Vandalism or fraud
Unauthorized access to and/or theft of software or data	Theft or trespass
Unauthorized use of computers and computer services	Petty theft, embezzlement, or joyriding

SOURCES: Office of Technology Assessment; and American Bar Association, "Report on Computer Crime, " 1984.

[1] National Criminal Justice Information and Statistics Service (now Bureau of Justice Statistics), U.S. Department of Justice, *Computer Crime: Criminal Justice Resource Manual, 1979.* (The report was produced by SRI International under contract). The terms "computer-related crime" and "computer crime" will be used interchangeably in this chapter for the sake of simplicity and adherence to current usage. Computer-related crime is, in a strict sense, more accurate, since in many cases the computer is not the central focus of crime, but rather a tool or a peripheral aspect. (Some would prefer the term "information crime, " since the important aspect of the act is not the effect on the machine, but the effect on the information it stores and manipulates.)

puter abuse as well as providing a recourse of last resort for those crimes that do occur.
- *Privacy* is related to computer crime in that such crimes may involve unauthorized access to personal information.
- *Intellectual property* issues are related to computer crime insofar as computerized piracy of software, for example, is a subset of computer crime more generally.[2]

The pivotal nature of computer crime makes it important to recognize these connections in the legislative process to ensure that Federal policies in these areas work in concert.

[2]A related Office of Technology Assessment study, "Intellectual Property Rights in an Age of Electronics and Information" (forthcoming in 1986), is examining these and related issues in detail.

BACKGROUND

The prime motivating factor for computer crime laws has been the increasingly widespread perception that current laws covering the variety of crimes that computer abuse resembles (e.g., fraud, theft, embezzlement, and trespass) either do not cover some abuses, or are not strong and clear enough to discourage computer crimes and allow expeditious prosecution.[3]

It is important to distinguish at the outset between computer crimes committed by outsiders who penetrate a system through communication lines (commonly known as "hackers "[4]) and crimes committed by insiders who are authorized to use the computer. The hacker problem has aroused a great deal of media attention, and some of the motivation to finally take action on computer crime legislation seems to be rooted in this phenomenon. The Nation has at times been alternately amused and terrified by reports of teenaged computer hobbyists entering computer systems at Los Alamos National Laboratory, Memorial Sloan-Kettering Cancer Center, and many others. OTA's analysis has led to the following observations:

- There are important differences between hackers who are young experimenters and hobbyists and those who are well-financed, sometimes malicious criminals. There is no question that the significance of teenaged hackers has been overblown. Close examination of many of the incidents tends to reveal that little actual damage was done,[5] or that simple safeguards (e.g., better password control, or dial-back modems) could have prevented the incident. This leaves at least some responsibility in the hands of the system owners who chose not to take "due care" in using such safeguards.

[3]See, for example, House Judiciary Subcommittee on Crime hearings on Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Sept. 29, 1983, Nov. 10, 1983, and Mar. 28, 1984; Raymond Natter, Congressional Research Service, "Federal Criminal Jurisdiction Under S. 240, 96th Congress: The Computer Crime Bill,"' Mar. 5, 1979; Nancy Finn and Peter Finn, "Don't Rely On the Law To Stop Computer Crime, " *Computerworld*, Dec. 17, 1984.

[4]This chapter uses a working definition of hackers as outsiders who penetrate a computer system they are not authorized to use through communications lines. The etymology of the term is somewhat controversial. Different writers use the term "hacker" to refer to a skilled computer programmer, a computer addict who knows the computer intimately but cannot communicate well with people, or a gifted but sloppy programmer.

[5]Many incidents of computer hacking have resulted in reports of many thousands of dollars in damages, and some incidents doubtless have caused delays and damage. The quantitative estimates of damage are difficult to evaluate, however, because they may include, for example, the costs *of* damaging publicity about the incident (which are somewhat speculative), or the costs of installing system security measures to prevent an incident from recurring (which are not "damages" but preventive measures that arguably should have been taken before the original incident occurred).

- Nevertheless, there is a growing segment of hacking that is more serious. Some of the reports of crimes committed by hackers seem to indicate a growing level of harm, and there are some reports of increasing involvement of organized crime in hacking, for example.[6] Thus hacking cannot be ignored as a component of the computer crime problem.
- However, as discussed in the previous chapter, computer and security experts are nearly unanimous in their view that the significance of outside penetration into computer systems pales in comparison with abuses by insiders who are authorized to use the computer. Like other kinds of white-collar crime, many of these incidents probably are not reported to law enforcement authorities. External threats may grow in severity, however, as computers are more and more frequently linked by telecommunications systems.

Thus, in designing effective legislation, it is essential to keep in mind the "insider' crimes that have recently received considerably less public attention than have hackers.

Legislative interest. The 94th Congress was the first to consider the subject of computer crime.[7] In addition to several celebrated frauds affecting the private sector in the early 1970s, a 1976 report of the General Accounting Office identified 69 instances of computer-related crimes affecting Federal programs, with resulting losses of over $2 millions

Senator Abraham Ribicoff, Chairman of the Senate Committee on Government Operations (now Governmental Affairs), first introduced the "Federal Computer Systems Protection Act of 1977" in the 95th Congress, and then sent a modified version of the so-called "Ribicoff bill" to the 96th Congress. The bill defined crimes related to:

- the introduction of fraudulent records or data into a computer system;
- the unauthorized use of computer-related facilities;
- the alteration or destruction of information or records; and
- the stealing, whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable data.[9]

Neither the 95th nor the 96th Congresses took final action on this proposal; one of the chief barriers was a concern that the bill expanded Federal jurisdiction too broadly. Since these groundbreaking efforts in this area, both the Congress and State legislatures have considered a myriad of bills, many of them patterned after Ribicoff's original effort. As of late 1985, 45 States have some kind of computer crime Legislation.[10]" Representative Bill Nelson, after helping to pass an innovative computer crime bill in the Florida State legislature in 1978, introduced a modified version of the Ribicoff bill in the 97th Congress (H.R. 3970, The Federal Computer Systems Protection Act of 1981).[11]

"Dorm B. Parker and John F. Maxfield, "The Nature and Extent of Electronic Computer Intrusion, " paper prepared for National Science Foundation Workshop on "Protection of Computer Systems and Software, " Oct. 19, 1984.

'See, for example, Senate Committee on Government Operations, *Problems Associated With Computer Technology in Federal Programs and Private Industry: Computer Abuses,* June 1976.

'U.S. General Accounting Office, "Computer-Related Crimes in Federal Programs, " Apr. 27, 1976, FGMSD-76-27. The most famous computer-related crime of the early 1970s was the "Equity Funding" scandal of 1973. Although the fraud did not involve any sophisticated manipulations of a computer, a computer system was used to generate $2.1 billion in fictitious policies. The fraud was based on a pyramid scheme, in which funds from new investors were used to pay off old ones.

"Louise Becker, *Computer Abuse and Misuse,* Institute for Defense Analyses, December 1984, p. 29. This document also summarizes the legislative history.

"'Jay Bloombecker, National Center for Computer Crime Data, Los Angeles, CA, personal communication, February 1986. The five States Bloombecker reports that do not have computer crime laws are New York, Vermont, West Virginia, Indiana, and Arkansas. The District of Columbia's computer crime law is also still under consideration. Bloombecker also reports that three States (Massachusetts, Maine, and Ohio) that are included in the total of 45 made only a minor modification to their criminal code to include data or computer services in the definition of property or services that can be the subject of theft.

"The innovative aspect of Florida's computer crime bill is that it defines two new classes of offenses: an offense against intellectual property, and an offense against the authorized computer user. (Finn and Finn, op. cit.)

As interest intensified (in part because of media reports concerning hackers), the 98th Congress considered at least 10 different legislative measures related to computer crime. (See table 5-2 for the titles and essential aspects of the bills proposed in the 98th Congress.)

Ultimately, under the leadership of Representative William Hughes, Chairman of the House Committee on the Judiciary, Subcommittee on Crime, and sponsor of H.R. 5616, the 98th Congress in its final hours passed an amended version of H.R. 5616 as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. (This will be referred to in this chapter as the Computer Fraud Act.) In drafting the bill, Representative Hughes focused on "trespass"—i.e., unauthorized access to specific kinds of information, rather than focusing on the "mere use" of the computer to commit an offense." Thus, the bill provides a felony penalty for unauthorized access to classified information, and a misdemeanor penalty for unauthorized access to the computerized information of financial institutions or the Federal Government. Two further sections of H.R. 5616 that covered any conduct that "affects interstate or foreign commerce" were deleted in final negotiations with the Sen-

'-House Report 98-894 to accompany H.R. 5616, July 24, 1984, p. 20.

Table 5-2.—The 98th Congress: Essential Characteristics of Computer Crime Bills

Bill	Action in 98th Congress	Jurisdiction	Important features
Counterfeit Access and Cornputer Fraud and Abuse Act of i984. Public Law 98-473 (H. R 5616, Rep. Hughes)	Passed in continuing resolution, hearings held by House Judiciary Subcommittee on Crime, 9/29/83; 11/10/83, 3128184	1) Classified information 2) Federal information systems 3) Financial institution information (deleted sections covering systems affecting interstate commerce)	Oriented toward "trespass,' i.e., improper access to the kinds of information defined at left. Gives Secret Service joint investigative authority
Federal Computer Systems Protection Act of 1984 (intro duced for the Administration by Sen. Thurmond, S. 2940)	Referred to Senate Judiciary	1) Government computer systems 2) Financial institution computers 3) Crimes involving two or more computers in different States (or countries)	Oriented toward using computer for fraud, damage to systems, unauthorized access. Includes forfeiture of interest in equipment used to perpetrate crime
Federal Computer Systems Protection Act of 1983 (HR. 1092, Rep. Nelson/S 1733, Sen Tnble)	Subject of hearing by House Judiciary Subcommittee on Civil & Constitutional Rights 11/18/83	1) Government computer systems 2) Financial institution computers 3) Computers used in interstate commerce	Oriented toward using computer for fraud, and damage to system or data. Derived from Ribicoff bill. Allows State jurisdiction to supersede Federal
Computer Crime Prevention Act of 1984 (S. 2270, Sen Cohen)	Referred to Senate Judiciary	1) Government computers 2) Financial institution computers 3) Computers used in interstate commerce	Oriented toward fraud, damage, unauthorized use. Same State role as H.R. 1092
Medical Records Protection Act of 1984 (HR. 4954, Rep Wyden)	Hearings by House Energy & Commerce, House Judiciary Subcommittee on Civil & Constitutional Rights, 416184, 819184	1) Medical records	Unauthorized access—misdemeanor; unauthorized access and tampering—felony
HR. 4384 (Rep, Mica)	Hearings by House Judiciary, Subcommittee on Civil & Constitutional Rights 11/18/83	1) Government computer systems 2) Financial institution computers 3) Computers used in interstate commerce	Incorporated H.R. 1092 but also sets up computer security research and interagency committee on computer crime
HR. 4301 (Rep. Coughlin)	Hearings by House Judiciary Subcommittee on Civil & Constitutional Rights 11/18/83	1) Interstate or foreign commerce	3-paragraph bill with harsh penalties for abuse
Small Business Computer Security and Education Act of 1984, Public Law 98-362 (H.R. 3075, Rep. Wyden; S. 1920, Sen. Tsongas)	Passed, hearings by House Judiciary Subcommittee on Anti-trust, 7/14/83, Senate Small Business, 317184	1) Small business	Provides information to small businesses to protect them from computer abuse. Establishes council to advise SBA on computer crimes
Amendment 7101 (Senators Leahy, Mathias, Kennedy, Baker)	Passed by Senate Oct. 11, 1984; dropped in conference	1) Privacy data (restricting Hughes bill jurisdiction over Federal information)	See text for discussion

SOURCES Office of Technology Assessment, using bill texts and hearing reports; and L Becker, ***Computer Fraud and Abuse,*** December 1984

ate. One clause would have provided a felony penalty for unauthorized access for the purpose of deliberate fraud resulting in a gain of $5,000 or more within a l-year period; the other would have provided a misdemeanor penalty for any unauthorized access to computerized information causing a $5,000 gain (for the defendant) or loss (for another) in a 1-year period.

The 98th Congress also passed the Small Business Computer Security and Education Act of 1984, which provides information to small businesses to protect them from computer abuse. While this act does not establish criminal sanctions for computer crimes, its advisory mechanisms could provide further information to help assess the magnitude of the computer crime problem.

In the 99th Congress, there has been substantial interest in further legislative action in this area. Several of the key lawmakers from the debates in the 98th Congress have introduced bills to supplement or change the Computer Fraud Act, as noted in table 5-3, and two other hearings have been held on the topic.[13] The actions proposed in the 99th Congress respond to three major sets of concerns about the Computer Fraud Act:

1. A variety of lawmakers and stakeholders have argued that Federal law should cover interstate private sector computer crimes in some way. H.R. 1001, introduced by Representative Hughes, reintroduces the sections on this topic deleted from the original H.R. 5616. Several of the other measures, H.R. 930 and S. 440, as well as the Administration's bill, H.R. 3381/S. 1678, also expand the law to cover interstate crimes.
2. Some analysts, principally in the civil liberties community, have expressed a concern that the wording of Section 3 of the Computer Fraud Act (specifically the outlawing of unauthorized disclosure of in-

[13] "House Judiciary Subcommittee on Crime, Hearing on H.R. 1001 and H.R. 930, May 23, 1985; and Senate Judiciary Subcommittee on Criminal Law, Hearing on Computer Fraud Legislation, Oct. 30, 1985,

Table 5-3.—The 99th Congress: Essential Characteristics of Proposed Legislation

Bill	Important features	Action in 99th Congress
Counterfeit Access Device and Computer Fraud and Abuse Act of 1985 [amendment] (H.R. 1001, Rep. Hughes)	Revises the act to add conduct "affecting interstate commerce, " wording that was deleted from original bill	House Judiciary Subcommittee on Crime held hearings 5/23/85
Computer Systems Protection Act of 1985 (S 440, Sen, Trible)	Defines jurisdiction to include computers that "operate in, or use a facility of, interstate or foreign commerce. " Includes limitation mechanism on Federal jurisdiction, refines definitions	Senate Judiciary Subcommittee on Criminal Law held hearings 10/30/85. Committee also requested comment from Justice and Treasury Departments
National Computer Systems Protection Act of 1985 (H. R. 930, Rep. Nelson)	Similar to above	House Judiciary Subcommittee on Crime held hearings 5/23/85
Medical Records Protection Act of 1984 (H.R. 995, Rep. Wyden)	Affects unauthorized access to medical records through telecommunications device. Provides misdemeanor for access, felony for tampering	Referred to House Energy and Commerce and House Judiciary Committees
S. 610 (Senators Mathias, Leahy, Kennedy, and Cohen)	Amends the act to make unauthorized disclosure of Federal computerized information a crime only if information is covered by the Privacy Act	Referred to Senate Judiciary, Subcommittees on Constitution and on Criminal Law. Committee requested comment from Justice Department
Federal Computer System Protection Act of 1985 (S. 1678, Sen. Thurmond; H.R. 3381, Rep. McCollum)	Administration bill. Outlaws use of computer to commit fraud, contains forfeiture provision for those convicted	Senate Judiciary Subcommittee on Criminal Law held hearings 10/30/85
Computer Pornography and Child Exploitation Prevention Act of 1985 (S. 1305, Sen. Trible)	Prohibits transmission of lewd or obscene material via computer, especially child pornography	Senate Judiciary Subcommittee on Juvenile Justice held hearings 10/1/85

SOURCE Office of Technology Assessment Compiled January 1986

formation *in* Federal Government computers) could be used to restrict informal information flows from government employees to the public or the press. During the 98th Congress, the Senate amended this portion of the bill to restrict its scope so that a person could only be prosecuted for unauthorized disclosure of personal (Privacy Act) information. However, this amendment was not incorporated in the final version of the bill. In the 99th Congress, S. 610 reintroduces this amendment.

3. Some congressional witnesses have argued that the act does not define crimes in a way that is clear and useful for prosecutors, and that the penalties specified—misdemeanors except for crimes involving classified information—are inadequate. (See discussion below.)

In addition, there appears to be substantial congressional interest in the related area of electronic eavesdropping and surveillance, as a result of H.R. 3378 and S. 1667, the Electronic Communications Privacy Act of 1985, introduced by Representative Robert Kastenmeier and Senator Patrick Leahy. The bill would extend legal protections currently applied to voice transmissions to virtually all electronic communications regardless of how they are transmitted. It also makes it a crime to obtain unauthorized access to electronic communications while they are stored in the computer of an electronic communication service, essentially a company providing message-handling services for electronic mail. Thus the bill would make two additions to computer crime law—protecting theft of data while it is being transmitted, and protecting messages in electronic mail systems. However, the bill does not protect stored data that is not associated with an electronic mail or communication system, which is the principal focus of the laws discussed in this chapter.*

As legislative discussion on computer crime has progressed, many key issues and questions have come into focus. In some cases, policymakers and stakeholders seem to be nearing consensus; in others, there are clear differences in approach with which Congress must grapple. The following sections describe some of these areas of agreement and disagreement, and discuss opportunities for further action.

*Fo, further discussion relevant to H.R. 3378 and S. 1667, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surt'eillance and Civil Liberties, OTA-CIT-293* (Washington, DC: U.S. Government Printing Office, October 1985).

MAJOR FINDINGS

Finding 1

There is a scarcity of reliable information about the amount of computer crime occurring and the nature and severity of the crimes. The available evidence suggests significant losses, though the full extent is unknown.

Recently, considerable attention has been focused on computer crime, particularly the small component of such activity that is committed by teenaged hackers.[14] Beyond anecdotes provided by the media, a number of organizations have attempted to develop evidence about the nature and scope of computer crime. Some of the highlights of these *studies are* reported below, with the caveats that each was limited in scope, was the first study of its kind, and had significant methodological flaws. Thus, the data and descriptions provided below represent only an impressionistic sketch of the computer crime situation, not an authoritative picture. The policy discussion at the end of this chapter will discuss needs for further information about computer crime.

The *American Bar Association (ABA)*[15] surveyed public and private sector organizations

"For examples of such attention, note Newsweek coverage of computer crime (Sept. 5, 1983, pp. 42-48; and Aug. 29, 1983, pp. 45-49): and the movie "War Games. "

"'Report on Computer Crime, " Task Force on Computer Crime, Section on Criminal Justice, 1984. Also see analysis in Louise Becker, *Computer Fraud and Abuse,* Institute for Defense Analyses, December 1984.

for their views on and experiences with computer crime.[16] Twenty-five percent (72) of the respondents reported "known and verifiable losses due to computer crime during the last 12 months." Fifty-four of the respondents reported that their total annual losses due to computer crime were between $0 and $100,000, while four respondents were in the $10 million to $50 million range, and one reported losses between $100 million and $500 million. The larger figures are staggering and, because the study was anonymous, cannot be substantiated. ABA notes that these figures cannot be extrapolated to the Nation as a whole and comments that many estimates of economic losses attributed to computer crime are "unexplained" and "unsupported."

The *American Institute of Certified Public Accountants*[17] conducted a survey of 5,127 banks and 1,232 insurance companies. Two percent (105) of the banks and 3 percent (40) of the insurance companies said they had experienced at least one case of fraud related to electronic data processing (EDP), a dramatically lower proportion of crime incidence than the ABA study although the methodology for the two studies is quite different. The study was not intended to provide reliable data on the incidence or the magnitude of frauds in insurance or banking, but rather to analyze the "general nature and means of committing some EDP-related frauds." Table 5-4 indicates some of the schemes reported for these frauds, from most to least frequent. The most frequent perpetrators of these frauds were clerical personnel (for smaller frauds) and mid-level management or supervisory personnel (for larger frauds). Only 16 percent of the frauds were reported to involve more than $100,000, and that figure does not reflect any funds recovered.

Table 5-4.—Commonly Reported Computer Crime Schemes in the AICPA's Study
(from most to least frequent)

Banking	Insurance
• Divert customer funds into perpetrator's own account	• Create fictitious claims
• Make unauthorized extensions of credit limits, loan due dates	• Trigger unauthorized refund or reduction of premiums
• Create fictitious loans	• Create unauthorized policy loans
• Defer recording of perpetrator's own checks and charges	• Trigger unauthorized dividend withdrawals
• Forge customer input documents (checks and withdrawals)	• Forge checks
• Make ATM extractions	• Create unauthorized mortgage loans
• Make adjustments to customer deposits	• Reinstate lapsed policies
• Divert loan payments into perpetrator's own account	• Create fictitious pension payments
• Divert customer income to perpetrator's own account	
• Wire transfer	

SOURCE American Institute of Certified Public Accountants. EDP Fraud Rewew Task Force, "Report on the Study of EDP.Related Fraud in the Banking and Insurance Industries," 1984.

In 1983, the *President Council on Integrity and Efficiency* released a report on the first phase of a study on computer-related fraud and abuse. The panel surveyed Federal agencies and found a total of 172 relevant cases (69 fraud, 103 abuse). The losses in fraud cases ranged from $0 to $177,383, with the highest proportion in the $10,000 to $100,000 range. However, noting that many agencies do not keep reliable or systematic data in this area, the leader of the study told a congressional committee that:

> One overriding finding of this study is that we still do not know the scope of computer-related fraud and abuse in government.[a]

A follow-on study by the Inspector General of the Department of Health and Human Serv-

[16] According to congressional testimony, "The survey was sent to approximately 1,000 private organizations and government agencies, including the Fortune 500 companies, banks, insurance companies, financial services, brokerage firms, accounting firms, all major Federal departments and agencies, all State attorneys general, and a sample of district attorneys." Responses were received from 283 organizations. (Testimony of Joseph B. Tompkins, Jr., to House Subcommittee on Transportation, Aviation and Materials, Sept. 24, 1984).

[17] "American Institute of Certified Public Accountants, EDP Fraud Review Task Force, "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries,"' 1984.

[a] "Richard P. Kusserow, Inspector General, Department of Health and Human Services, testimony to House Subcommittee on Transportion, Aviation, and Materials, Sept. 24, 1984.

ices contained interviews and analyses of 46 perpetrators of computer-related fraud cases in the Federal Government. Although it is not known to what extent these perpetrators are representative, in general they:

- were insiders, and were typically young, well-regarded employees;
- held a wide variety of positions, although most commonly were caseworkers, clericals, or data-entry technicians;
- typically committed their crime by manipulating input data to cause funds to be issued, and most were aided by co-conspirators;
- committed the criminal activity over a 6-month period, on the average;
- stole in response to a situational stress, such as personal indebtedness; and
- didn't think about the consequences of their actions, or assessed the risks of getting caught as minimal. 'g

The *Department of Justice Bureau of Justice Statistics* (BJS) has commissioned various reports to try to assess the nature and scope of computer crime. One recent BJS report examined the scope of fraud related to electronic funds transfer in a confidential survey of 16 banks. Because of the small sample size, this pilot study's results should be viewed as suggestive only. The study estimated that banks nationwide lost $70 million to $100 million during 1983 from automatic teller fraud. This is only about 0.03 percent of a total volume of $262 billion processed through automatic tellers, or a loss of 32 cents per $1,000 of transaction volume. The study also examined potential losses from wire transfers, although there were insufficient data to estimate national loss levels. Twelve banks reported 139 wire transfer fraud incidents within the preceding 5 years, with an average exposure to loss (before recovery efforts) per incident of $883,279, and an average net loss (after recovery efforts) per incident of $18,861. By comparison, roughly 60 million wire transfers were completed in 1980, involving$117 trillion. [20]

Consultants and other researchers have also played significant roles in assessing the nature and scope of computer crime. In one recent study, two researchers conducted telephone interviews with 106 law enforcement officials and prosecutors in States that had computer crime statutes. Sixty-seven investigations under the new computer crime laws were identified, leading to 56 indictments and 32 convictions. The authors found:

- only a few of the many incidents investigated resulted in prosecution, primarily because the evidence available did not appear to support indictment. Some prosecutors reported that grand juries failed to understand the case because of the technical nature of the acts involved;
- more perpetrators now seem to be mounting a defense than did those prosecuted in the past. The most actively defended recent cases have been those involving electronic trespass;
- many prosecutors interviewed were unaware that their State had a computer crime law;
- some prosecutors reported that because penalties for violation of their computer crime laws are less than those for traditional theft and burglary laws, they favor use of the more stringent statutes; and
- many prosecutors chose to use the computer crime law only when a traditional fraud, theft, or malicious mischief statute was clearly less applicable. Therefore, this report likely covers only a small proportion of all computer crimes because of the preponderance of cases prosecuted under other laws. The most experienced prosecutor of computer crimes in California strongly supports this conclusion.[21]

SRI International has also kept a file of computer crime incidents, principally consisting of media reports. However, SRI's lead investigator in this area has for some time argued forcefully that none of the figures quoted on the subject of computer crime (including

"'Richard P. Kusserow, "Computer-Related Fraud in Government Agencies: Perpetrator Interviews, " published by the Department of Health and Human Services, May 1985.

"'Bureau of Justice Statistics Special Report NCJ-96666, "Electronic Fund Transfer Fraud, " March 1985.

'"Susan Nycum (Gaston Snow & Ely Bartlett), and Dorm Parker (SRI International), 'Prosecutorial Experience With State Computer Crime I.aws, " February 1985, pp. 15-16 (unpublished paper).

SRI's) are reliable." This researcher and another veteran of computer crime debates have written:

> No valid statistics representative of the computer crime problem currently exist. Although many estimates have been published and often quoted, investigation has shown that these are not representative, primarily because of the following:
>
> Ž Few victims are willing to report incidents and suffer the staff-time expense, embarrassment, civil liabilities, business disruption, questionable basis for litigation, and violation of security by revealing vulnerabilities.
>
> • Definitions of what constitutes a crime differ from state to state so that events cannot be consistently measured.
>
> . No successful collection mechanisms for statistics have been discovered and developed. . . .
>
> The lack of statistics measuring the size of the problem has been a source of concern. Although news media attention on spectacular individual cases has created the image of a very serious problem, the absence of valid data makes establishing rational legislative priorities and characterizing the problem difficult.[23]

In contrast, another prominent computer security expert argues that it is, in fact, quite possible to develop usable data on computer crime, although he acknowledges that "statistical analyses of data on computer-related crime do not lead to the predictability of such crime in any particular working environment. "[24] Of the 1,406 cases tracked by this author as a part of his role as a security consultant, he reports that there is an average loss of $500,000; that 89 percent are never taken to the criminal justice process; and that of the 11 percent that are, convictions are obtained in only 18 percent.[25]

The *Justice Department Fraud and Corruption Tracking (FACT) System,* begun in 1983 primarily to track cases involving fraud in the Federal Government, reported 8 computer-related crimes out of 3,112 fraud and corruption cases in 1983, and 18 out of 3,582 in 1984. The system includes only cases prosecuted by the FBI and those at agencies that Congress has mandated to be monitored under the FACT System. Most of the cases involved false data entry to get unauthorized benefits from unemployment or welfare programs.[26]

In short, only a few scattered pieces of information are available on computer crime; much of the quantitative information is analytically soft; and in some cases, the studies conflict with one another. Some of these studies, such as the ABA report, seem to suggest fairly widespread patterns of computer crime; some of the others indicate a significant amount of such criminal activity, but with the full extent unknown.

It is arguable how much could reliably be known about the nature and scope of computer crime. Like many other white-collar crimes, companies may not want to report these incidents to law enforcement agencies, particularly in the case of large losses that may result in embarrassment or exposure of vulnerabilities. However, it is possible that more focused study of computer crime could improve the soft information now available. For example, one congressional witness suggested that a large-scale "victimization study," undertaken by professional criminologists, could add substantially to knowledge in this area.[27] This issue will be discussed further at the end of this chapter.

"Donn"Parker, SRI International, OTA work session, Jan. 25, 1985.

[23] Nycum and Parker, op. cit., pp. 2-3.

"Robert Courtney, Jr., and Mary Anne Todd, "Problem Definition: An Essential Prerequisite to the Implementation of Security Measures, " paper prepared for presentation to The Second International Congress and Exhibition on Computer Security, Toronto, Sept. 10-12, 1984.

"Robert Courtney, Jr., Interview with OTA staff, July 17, 1985, Because Courtney does not divulge the details of his cases in order to preserve the anonymity of his clients, his data are not open to other expert scrutiny.

"Glenn McLaughlin, Congressional Research Service, Library of Congress, "Computer Security and Crime," Issue Brief IB85155, Oct. 22, 1985.

"Sanford Sherizen, testimony to Senate Small Business Committee, Mar. 7, 1984.

Finding 2

Despite the lack of hard information, the vulnerabilities of organizations using computer systems are much greater than in the past. Thus a consensus has emerged that a combination of Federal and State laws is appropriate in this area.

As discussed in chapter 4, rapidly changing technical and social factors have increased the risks and potential losses related to information systems by an order of magnitude. These changes include increased networking, the advent of microcomputers, increased dependence on information systems, and increased computer literacy. The increasing awareness of these new levels of risk, and resulting consensus in support of Federal legislative action, can be seen both in the actions of Congress (passing, without dissent, the Computer Fraud Act), in substantial testimony to Congress, and in the opinions of many experts and groups.[28]

This apparent consensus is a very significant change from earlier sentiment in Congress. In many of the earlier hearings on computer crime, the view was expressed that the existing network of statutes covering, for example, wire and mail fraud, embezzlement, and privacy should be adequate to cover computer crime, and/or that it should primarily be under State jurisdiction.[29]

While some might still debate this point, the Federal and State actions taken so far have, in essence, accepted the need for legislation, and set forth Federal and State roles in this area of crime—namely, that while State laws will play a primary role in most cases, Federal legislation will concentrate on areas of special Federal concern: e.g., Federal records, financial information, classified information, and possibly interstate crimes and medical records.

One potential problem with this de facto allocation of roles in the area of computer crime is that different State laws are frequently inconsistent. One legal expert has suggested that a body such as the National Conference of Commissioners on Uniform State Laws could focus on computer crime laws and possibly draft a uniform model State law.[30]

Finding 3

Legislation needs to balance concern about the potential urgency of the situation with other factors—in particular, the responsibilities of vendors, owners, and users for the security of their systems, and the need for keeping computer crime sanctions reasonably consistent with other criminal law.

Because the nature and value of intangible data are difficult to assess, and because it is often hard to distinguish myth from reality where computers are concerned, it is easy to overreact to stories about computer crime.

For example, computer professionals argue that many computer systems are irresponsibly left unprotected because simple precautions are not taken-the computerized equivalent of leaving piles of money in bank windows. Such simple precautions include, for example, requiring the authority of two persons for disbursements, maintaining logs of system activity and scanning them for unusual patterns, changing standard passwords that are set for every system when they are first turned on, or using "dial-back" modems that require users to be at their authorized terminal loca-

[28] See, for example, testimony to House Judiciary Subcommittee on Crime, Sept. 29, 1983, N'ov. 10, 1983, and Mar. 28, 1984; testimony to the House Science and Technology Subcommittee on Transportation, Aviation, and Materials hearings on Computer and Communications Security and Privacy. Sept. 24, 1984; and testimony to the Senate Governmental Affairs Subcommittee on Oversight of Government Management, "Computer Security in the Federal Government and the Private Sector, " Oct. 25-26, 1983. The American Bar Association and American Institute of Certified Public Accountants reports cited previously also argue forcefully for legislative action, In addition, the Data Processing Management Association, Videotex Industry Association, and Information Industry Association have each drafted model computer crime bills and urged Federal computer crime legislation, The Computer and Business Equipment Llanufacturer's Association supported Representative Nelson's bill, H.R. 1092. And, a 1983 survey of 637 members of the American Society for Industrial Security indicated that 93 percent of the respondents felt a need for computer crime legislation at the Federal level (presented in Senate hearings, above, p.163). Also see Finding 1 and discussion in ch. 4.

[29] See, for example, Senate Judiciary Subcommittee on Criminal Justice, "Hearings on S. 240, Computer Systems Protection Act of 1979, " Sept. 23. 1982.

[30] Daniel Burk, "The Philosophies of Computer Crime Legislation: An Editorial Collection, " *Computer Law Reporter,* vol. 3, No. 3, November 1984.

tions. (See ch. 4 for further discussion of security measures.) Thus, some would argue that the urgency of the need for computer crime legislation is considerably less than commonly perceived because of these systems that are left irresponsibly unprotected."

This is not to say that legislation is not needed. Car theft is illegal, for instance, even though many people leave their car doors unlocked–but it does raise the importance of both the Federal Government and the private sector pursuing computer security at the same time that computer crime law is being developed. That is, legislation alone is not a solution to computer crime. These relationships be tween computer security and computer crime highlight the need for Congress to coordinate its efforts in examining the two topics.

Further, as noted earlier, the gravity of many of the incidents of computer hacking has been exaggerated. For instance, the system that hackers broke into at Los Alamos National Laboratory in 1984 was new and still undergoing testing.[32] In fact, one participant in OTA'S work session on information security, whose views are shared by many in the computer science research community, argued that we should not discourage young people from hacking:

> A lot of the people who are known as pretty good programmers started out as hackers 15 or 20 years ago poking around in systems be cause that was the only option available. In many respects that was also the best thing we could do for our society, which after all built its mid-century experience on whole generations of people who learned auto mechanics souping up their cars to violate the speed laws.
>
> This poking around used to encourage teenagers to go into computing. And if the lure of a little illicit playing around in somebody else's computer is doing that, the benefits for our society are going to far outweigh the inconvenience of having a few people who weren't careful enough and had their files damaged by inexperienced people playing around on the computers.[33]

This view is quite controversial, although significant as a counterpoint to other voices that argue for strict computer crime laws. It should be interpreted in the spirit in which it was intended—as a warning against excessive penalties for nonmalicious experimentation, not as an argument that criminals who use computer hacking to commit crimes should be sanctioned by the law. And clearly there are some systems in which experimentation is more tolerable than others—at schools of computer science, for example, where hacking is even tacitly encouraged—while there are others that are far more sensitive and should be well protected, both by law and by security measures.

A second important broad concern is the need for keeping standards and practices for computer crime reasonably consistent with standards and practices for other kinds of criminal activity. For example, one scientist compared an employee "stealing" computer time to do personal work (a much discussed form of computer abuse in computer literature and congressional hearings) to a machine tool operator who uses the shop's equipment after hours for personal work. The policy for such activity varies among machine shops from forbidden to encouraged, but it is generally not considered a criminal offense.[34]

Finally, it is worth noting that there are potential disadvantages to being overzealous in computer crime legislation. This is related to a question that Senator Paul Laxalt raised in 1980 hearings:

> By focusing on the computer as an instrumentality, are we exposing individuals to criminal liability for possibly innocent conduct while not furthering the public safety?

Previous OTA testimony also warns against "criminalizing bad manners":

[31] OTA work session on information security, Jan. 25, 1985.
[32] Suzanne Smith, Los Alamos National Laboratory, Remarks to Air Force Federal Information Systems Risk Analysis Workshop, Montgomery, AL, Jan. 22, 1985.
[33] OTA work session, Jan. 25, 1985.
[34] The Computer Fraud Act does not criminalize the unauthorized use of computer time for personal purposes, although some State statutes do.

> Not all instances of unethical behavior are illegal. Behavior such as eavesdropping on private conversations and snooping into private papers by individuals is not totally covered by law. Instead, society regulates it through a less formal system of social rewards and punishments. As communications increasingly take electronic form and as laws and regulations are passed, such behavior may become subject to formal criminal rather than informal social sanction. Maybe in many cases it should be treated so, but we may need to build sufficient flexibility into the law to avoid criminalizing all bad manners.[35]

Overly restrictive or intimidating legislation could also, for example, stifle productive flows of information from government to the public, or stifle productive and creative activities on the part of computer users. Several critics of the Computer Fraud Act have argued that the law could be used by agencies bent on secrecy to prosecute employees for informally divulging computer-based information to the public or the press—even if that information was available to the public under the Freedom of Information Act.[36]

Finding 4

> A number of possible actions have been identified to clarif y and/or strengthen the Federal role in monitoring, preventing, and prosecuting computer crime. Congress has already enacted computer crime legislation,[37] but there are a substantial number of proposals before the 99th Congress to fine-tune or change the Computer Fraud Act in some way (see table 5-3).

Congressional witnesses and others have raised several important doubts about the adequacy of the new act for effective prosecution of violators, based on the limited experience currently available. Two major problems reported by prosecutors are:

1. the fact that the act only provides for misdemeanor penalties unless the information accessed is classified. This may not be sufficient incentive to proceed with a criminal case; and
2. the act's wording, which defines a crime as an unauthorized access that "affects" a government or financial institution computer. Some argue that "affect" is a vague and overly broad terms[38]

The legislative debate and hearings have identified several actions that could strengthen and/or clarify the Federal role in monitoring, preventing, and/or prosecuting computer crime. These are discussed briefly below.

Extend the Federal statute to cover interstate crimes affecting private sector computers.

In part because of considerable variation in State laws governing computer crime (and because a few States still do not have computer crime laws), a Federal statute could clarify and standardize policies for interstate crimes. However, the definition of "interstate" needs to be carefully examined. Several of the computer crime bills cover systems that "affect interstate or foreign commerce, "3[39] or "operate in, or use a facility of, interstate commerce. "4° This could cover a very large number of information systems and prospective crimes if Federal officials chose to interpret it that way. Many businesses routinely exchange information between their computers located in several States; almost all systems use a telecommunications carrier that operates across State lines. The Administration bill (S. 1678 in the 99th Congress), on the other hand, covers only crimes in which "two or more computers are used which are located in different States or in a State and a foreign country. " The Admin-

---

"Testimony of Frederick Weingarten, Program Manager, Communication and Information Technologies Program, Office of Technology Assessment, before the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice, "Electronic Surveillance and Civil Liberties," Oct. 24, 1985.

"New *York 7'imes,* "Computer Privacy, Not Secrecy, " Oct. 11, 1984; and Allan Adler and Jerry Berman, American Civil Liberties Union (ACLU) Memo on "Need to Revise Newly Enacted Computer Crime Statute, " January 1985.

[37] See table 5-2. Both the Counterfeit Access and Computer Fraud and Abuse Act of 1984 (Public Law 98-473) and the Small Business Computer Security and Education Act of 1984 (Public Law 98-362) were enacted in the 98th Congress.

[38] See May 23, 1985, hearing of the House Judiciary Committee, Subcommittee on Crime, on "H. R. 1001 and H.R. 930, Bills relating to Computer Crime and Computer Security"; and Mitch Betts, "U.S. Attorneys Push To Clarify Vague '84 DP Crime Law, " *Computerworld,* July 1, 1985.

[39] H.R. 1001 in the 99th Congress, Representative Hughes.

[40] S. 2270 in the 98th Congress, Senator Cohen.

istration wants a limited Federal role in the area of computer crime, in line with its understanding of Federal/State roles.[41]

Because of the fluid nature of telecommunication networks, computerized information may cross State lines in transmission even if the perpetrator is in the same State as the host/victim computer. Thus, in general, establishing the site of the computer crime, and hence the jurisdiction, can be difficult. Because of this difficulty, OTA found that it would be useful to have broad wording for the definition of "interstate" in Federal computer crime cases, while at the same time providing a checking mechanism so that Federal jurisdiction does not expand without bounds. Several bills provide for Federal jurisdiction while adding such a mechanism by allowing State jurisdiction to supersede Federal under certain conditions, through a careful weighing of priorities and Federal interest in the case.[42] Another advantage of providing this option for State officials is that they can use the expertise of the FBI or Secret Service if necessary; Federal involvement could also help to standardize State treatment of computer crime cases. To further standardize State approaches to computer crimes, Congress may also wish to commission or participate in the development of a model State computer crime act, as discussed earlier.[43]

Amend the conceptual approach to defining computer crime used in the Computer Fraud Act.

There are at least two basic ways legislation could define computer crimes and address sanctions:

1. laws could declare it a crime to access certain kinds of information or to make unauthorized use of the machine itself essentially a kind of *trespass;* or
2. laws could concentrate on the nature of the crime committed while using a computer, essentially a *tool* approach.

The Computer Fraud Act and Representative Hughes' proposed amendment in the 99th Congress, H.R. 1001, both take the trespass approach because they define crimes according to unauthorized access to particular types of information, or unauthorized use of computers (in H.R. 1001, for interstate computer crime). Most of the other bills take the "tool" approach, focusing on use of the computer to defraud. This approach does not require that prosecutors prove access was unauthorized, which can be difficult for insider crimes.

An interesting variation on the "tool" approach are model computer crime acts drafted by the Videotex Industry Association and Data Processing Management Association in 1984; these model acts define different kinds of crimes such as "computer fraud, " "damage or destruction of computer property, " "computer trespass, " and "theft of computer property or services. " The Virginia computer crime act adopts this approach, defining five new crimes: computer fraud, computer trespass, computer invasion of privacy, theft of computer services, and personal trespass by computer.[44] These categories are similar to those outlined earlier in table 5-1.

"Statement of John C. Keeney, Deputy Assistant Attorney General, Criminal Division, Department of Justice, to House Judiciary Subcommittee on Civil and Constitutional Rights hearings, Aug. 9, 1984.

"The Nelson (H.R. 930 in the 99th Congress), Trible (S. 440 in the 99th Congress), and Cohen (S. 2270 in the 98th Congress) bills have this provision. They say that in cases of concurrent Federal and State or local jurisdiction, Federal law enforcement officers should consider the relative gravity of the Federal offense and the State or local offense; the relative interest in Federal investigation or prosecution; the resources available to the Federal authorities and the State or local authorities; the traditional role of the Federal authorities and the State or local authorities with respect to the offense; the interests of federalism; and any other relevant factor. (S. 440, Section 6b.) These bills also provide for periodic reports to Congress on the effect of the law on the scope of Federal jurisdiction. The provisions for balancing State and Federal interests in establishing jurisdiction are already reflected to some extent in internal Department of Justice policies. (Ed O'Connell, House Judiciary Subcommittee on Crime, personal communication, January 1986.)

"For good analyses of some of the differences between State laws in this area, see Becker, op. cit., and Nycum and Parker, op. cit.

"Virginia Computer Crimes Act, Virginia Code Section 18.2 -152.1 et seq., signed by the Governor Apr. 11, 1984. The act also expands the definition of embezzlement in Virginia's criminal code to include embezzlement of computer time and services. For a discussion see Daniel Burk, "Virginia's Response to Computer Abuses: An Act in Five Crimes, " *Computer Law Reporter,* July 1984.

Because this kind of "tool" approach connects computer crimes closely to traditional (noncomputer) violations that the computer crimes resemble, it may be easier for many people (and perhaps prosecutors) to understand. However, sentiment in the 99th Congress, as evidenced by the proposed legislation, is either to retain the conceptual framework of the Computer Fraud Act with some additions or modifications, or to adopt a simplified "tool" approach. The Administration's bill essentially uses this latter approach, focusing on fraud or theft committed with the computer.

Change the kinds of information covered in Federal legislatiom to include medical records, to clarify the law regarding disclosure of public information, and/or to clarify the definition of "financial institution."

Three possible changes have been clearly identified. One would extend coverage to include medical records. Interest in this measure was aroused by reports of a hacker break-in at Memorial Sloan-Kettering Cancer Center in New York in 1983.[45] However, the relative frequency and seriousness of threats to medical records have not received close study. The Administration argues that tampering with medical records should be considered an issue of State law, unless the records are those of a Federal agency or Federal medical facility.[46]

The second potential change in the kinds of information covered in the Computer Fraud Act is the option of restricting the kinds of information covered in section 3 (Federal records). S. 610 modifies subsection a(3) of the Computer Fraud Act; while it is still a crime to modify, destroy, or use Federal information, the disclosure of information is outlawed only if the information is protected by the Privacy Act. As mentioned earlier, Senators Leahy, Mathias, Kennedy, and Baker,[47] civil liberties advocates,[48] and others argued that making a crime of unauthorized access and disclosure of any Federal computerized information would restrict Congress and the public's access to information whose disclosure is not restricted if it were not in a computer. While Representative Hughes has asserted that this should not be a problem since a "whistleblower" or other Federal employee who wanted to pass on information informally would have authorized access to the computer, conceivably the agency involved could argue that the disclosure was a "purpose for which such authorization does not extend." OTA found that restricting the unauthorized disclosure phrasing in this paragraph could help clarify the statute, and deserves careful consideration.

Third, the Department of Justice'[49] has testified that the definitions of financial information protected by the 1984 Computer Fraud Act are unwise because they restrict coverage to financial records as defined by the Right to Financial Privacy Act of 1976, or credit agency records as defined in the Fair Credit Reporting Act. Thus, in the Justice Department interpretation, the act's definition excludes the bank's own records, as well as records on corporations. The Administration bill would cover frauds or thefts perpetrated with access to any financial institution computer.[50]

[45] See Representative Wyden's testimony to House Judiciary Civil and Constitutional Rights Subcommittee, Aug. 9, 1984.

[46] John C. Keeney, Deputy Assistant Attorney General, testimony, Subcommittee on Civil and Constitutional Rights, Aug. 9, 1984.

[47] *Congressional Record,* Oct. 11, 1984, pp. S14403, S14445.

[48] See ACLU memo, and *New York Times,* op. cit.

[49] Victoria Toensing, Deputy Assistant Attorney General, Criminal Division, Department of Justice, testimony before the House Judiciary Subcommittee on Crime, Oct. 30, 1985.

[50] A related piece of legislation, the Computer Pornography and Child Exploitation Prevention Act of 1985 would criminalize use of a computer to transmit obscene, lewd, or lascivious writing, descriptions or pictures, or information pertaining to sexual exploitation of children. While preventing exploitation of children is clearly a desirable goal, defining obscenity by computer is no easier than defining it in other media, and keeping standards for "electronic pornography" reasonably consistent with other laws and social standards, such as first amendment rights to free expression, is difficult. A full analysis of this legislation is beyond the scope of this report. (See, for example, Mitch Betts, "Regulation of Bulletin Boards Faces Strong Opposition," *Computerworld,* Sept. 9, 1985; T.R. *Reid,* "Big Brother Trible Has His Eye on Your Personal Computer," *The Washington Post/Washington Business,* Sept. 16, 1985, p. 5.) For arguments in favor of this legislation, see testimony presented at the Oct. 1, 1985, hearing of the Senate Committee on the Judiciary, Subcommittee on Juvenile Justice.

Establish strengthened or new reporting systems for monitoring computer crime.

The Department of Justice and FBI, for example, could further expand their ability to develop effective statistics on computer crime, or could conductor sponsor further studies of the topic. Although there have been several efforts to develop information about computer crime, the resulting information is unsatisfactory from the point of view of legislators trying to judge the severity of a problem. There are two aspects to this problem—information about the pervasiveness of computer crime in society and business generally, and specific information about computer crimes within the Federal Government.

Based on the weaknesses of current studies as discussed in Finding 1, OTA found that a further effort to assess the nature and scope of computer crime in society and business generally would be most worthwhile if the effort:

- is large-scale, well-funded, and run by a credible and impartial organization, so that the results will be authoritative;
- includes both quantitative studies of the scope of computer crime and qualitative information on the nature of the crimes, how they are evolving, and what influences organizations in deciding whether to prosecute;
- includes the expertise of professional criminologists who have developed relatively sophisticated techniques for interviewing victims of crime;
- compares computer crimes to other forms of white-collar crime in nature, evolution, and prosecution aspects;
- compares an organization's susceptibility to computer crime to its computer security measures; and
- guarantees the anonymity of the victim organizations contacted.

In addition to such a study of computer crime in general, Congress could direct further studies of such crime within the Federal Government. There are several good beginnings toward collecting such data—e.g., the two reports issued by Richard Kusserow, Inspector General of the Department of Health and Human Services; and the Fraud and Corruption Tracking System at the Department of Justice. However, only 19 percent (25 of 130) of agencies responding to OTA's Federal Agency Data Request reported that they had an established procedure for tracking and analyzing computer crime within their agency. Such procedures could be mandated.

Other actions that have been suggested include:
–Clarifying the definition of "authorization" in the Computer Fraud Act.

This could help make the Computer Fraud Act clearer since this concept underlies the whole statute. A definition proposed as an amendment to the Virginia statute (although not yet taken up by the legislature) could be a useful starting point:

> A person is "without authority" when he has no right or permission of the owner and no reasonable grounds to believe that he has such right or permission, or, he exceeds such right or permission. It shall be an affirmative defense to a prosecution under this act that: 1) the person reasonably believes that the owner, or a person empowered by the owner, has given authority to that person; 2) the person reasonably believes that the owner, or a person empowered by the owner, would have given authority without payment of any consideration; or 3) the person reasonably could not have known that he was without authority.[61]

–Enacting a limited provision to protect competitive secrets of victim organizations during prosecution, in order to encourage prosecution of computer crime.

Since a key reason why companies do not prosecute computer crimes is a concern that they will expose vulnerabilities or competitive secrets during the litigation process, Congress

[61] "Virginia House Bill 1469, proposed on Jan. 21, 1985, as an amendment to Virginia Code Section 18.2-152.2, The Connecticut computer crime bill, Public Act 84-206, Section 2(b)(l), passed Oct. 1, 1984, uses essentially the same definition.

may wish to consider a clause that would allow some portion of the criminal proceedings to be protected. Clearly, there are trade-offs for establishing such a provision in the law, and it is important to guard against infringement of the right to an open trial. A clause that was proposed for the District of Columbia computer crime act could serve as a model."

–Enacting a penalty for persons convicted of a computer crime that would include forfeiture of their interest in (i.e., confiscation of) equipment used in the crime.

A provision to this effect was included in the Administration's bill, but not in the Computer Fraud Act. The Administration argues that such a provision would be a powerful disincentive to hackers and an appropriate penalty for those who might not otherwise receive prison sentences or "meaningful fines."[53] Federal law has traditionally included only very limited forfeiture provisions, principally for drug and racketeering crimes. The effectiveness of a forfeiture provision in discouraging hacking has not been closely examined. One of the factors that would seriously hinder its effectiveness is that teenaged hackers frequently do not own the computer equipment that they use to commit a crime; adult hackers often use machines at their place of employment.

–Establishing a forum to address in a more systematic way the connections between computer crime, computer security, and Federal information policy.

The House Subcommittee on Transportation, Aviation, and Materials has recommended the formation of a national study commission to address these issues.[54] Similarly, Representative George Brown has, in several sessions, proposed the establishment of an Institute for Information Policy and Research to address national information policy issues. [55]

Such a commission or institute could help reinforce the connections between these topics, raise the visibility of a variety of information policy issues, and serve as an effective coordinator of studies, such as on the extent of computer crime. On the other hand, either a commission or an institute might delay action, and would incur some additional cost. However, proponents argue the work of a commission or institute could, in the long run, save far more than the direct cost. Several commissions have played major roles in shaping Federal policy in the issues discussed in this report, including the Commission on Federal Paperwork (which issued its final report in 1977), the panel associated with the Presidential Reorganization Project (1979), and the Privacy Protection Study Commission (1977). The first two are discussed further in chapter 2.

Any Federal effort should clearly draw from and work in concert with independent efforts in the private sector to examine these issues. For example, the American Federation of Information Processing Societies has formed a "National Information Issues Panel" to examine information policy issues and provide guidance to government leaders.[56]

"Daniel Burk, Cadwalader, Wickersham, and Taft, Washington, DC, personal communication, March 1985. The D.C. Government has not yet passed a computer crime law. The proposed clause reads in part: "The court may, in its discretion and upon good cause shown, conduct all criminal proceedings under this article in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets involved. The court's discretion under this section shall be exercised in such a way as to balance (a) the offender's important right to a public trial with (b) the District of Columbia's compelling public interests in avoiding the recurrence of the same or similar acts, in encouraging the prosecution of the crimes defined under this article, in encouraging complete and truthful testimony so that the offender is fully tried with all facts brought to the attention of the trier of fact, and in protecting the trade secrets of the owner, if any of such compelling interests are in fact present in the instant case. The court shall conduct only so much of the proceedings in secret as shall be absolutely necessary to promote these compelling interests of the District of Columbia."

[53] Toensing, op. cit.

[54] House Science and Technology Subcommittee on Transportation, Aviation, and Materials Report, "Computer and Communications Security and Privacy, April 1984.

"Information Science and Technology Act of 1985, H.R. 744 in the 99th Congress.

[56] American Federation of Information Processing Societies, Inc., "AFIPS Announces Formation of Panel on National Information Issues," news release, May 1985. The panel is chaired by Robert Lee Chartrand of the Congressional Research Service.