UIC John Marshall Journal of Information Technology & Privacy Law

Volume 1
Issue 1 *Computer/Law Journal*

Article 16

1978

On Computer Crime (Senate Bill S. 240), 1 Computer L.J. 517 (1978)

John K. Taber

ON COMPUTER CRIME (SENATE BILL S. 240)

*by John K. Taber**

INTRODUCTION

Now pending before Congress is Senate Bill S. 240,[1] introduced by Senator Abraham Ribicoff (D. Conn.) on January 25, 1979, and entitled "Federal Computer Systems Protection Act of 1979." This bill attempts to define and outlaw "computer" crimes.[2]

S. 240 consists of a preamble and three sections. The preamble asserts that computer crime is a growing, serious problem that is difficult to prosecute under existing laws, thus necessitating new federal legislation. Section (a) of the bill outlaws any use of a computer for fraudulent purposes. Section (b) outlaws "intentional, unauthorized" use, access, or alterations of a computer, computer programs or data. Section (c) contains definitions of various terms used in the bill.

The legislation covers all government computers, any computers used by private entities with government contracts, computers used in banking and finance, as well as all computers used by "any entity

---

* B.A. 1974, University of California, Berkeley; Systems Programmer, International Business Machines Corporation since 1970. Mr. Taber has worked on the development of APL (A Programming Language), and is currently working on the development of large data bases.

The author is very grateful to John S. James, Dr. Harry Saal, and Lawrence M. Breed, for their critical review of this article and their many helpful suggestions for improvement. The views expressed by the author are entirely his own and should not be construed as reflecting the views of any organization, or any other person. Errors also are entirely his own.

1. The text of S. 240 is reprinted in the Appendix to this article.

2. A virtually identical bill, S. 1766, was introduced by Senator Ribicoff in the Ninety-fifth Congress (123 CONG. REC. 10,790 (daily ed. June 27, 1977)), but failed to be reported out of the Senate Committee on the Judicary before the end of the second session. *See Federal Computer Systems Protection Act (S. 1766), Hearings Before the Subcomm. on Criminal Laws and Procedures, Comm. of the Judiciary*, 95th Cong., 2d Sess. (1976) [hereinafter cited as *Hearings*].

operating in or affecting interstate commerce."[3] The penalties for a violation of section (a) are fifteen years imprisonment and/or a fine of two and one-half times the amount stolen. For a violation of section (b), the penalties are fifteen years imprisonment or a $50,000 fine, or both.

The purpose of this article is to point out the fatal flaws that should preclude this bill from ever becoming law, and suggest that there is no such thing as a "computer" crime, and therefore no need for special legislation addressing this "problem."

I. COMPUTER CRIME: FACTS AND MYTHS

The rationale for this legislation, as presented in the bill's preamble,[4] has never been established. There is no evidence that computer-based fraud and embezzlement are increasing. In fact, losses from computer-related crimes are insignificant when compared with criminal losses in general,[5] and losses from so-called "white collar" crimes in particular.[6]

While almost everyone is aware of the sensational accounts of "computer crimes" contained in the mass media, these stories are, simply put, either grossly exaggerated or just plain wrong. For example, newspapers widely reported that the Security Pacific Bank theft in Los Angeles, California, was a "computer" crime;[7] it was not.[8] The Pennsylvania Railroad boxcar thefts were also reported as

---

3. S. 240, 96th Cong., 1st Sess. § 3(a) (1979).

4. The Congress finds that—

(1) computer-related crime is a growing problem in the Government and in the private sector;

(2) such crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;

(3) the opportunities for computer-related crimes in Federal programs, in financial institutions, and in other entities which operate in interstate commerce through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great;

(4) computer-related crime directed at institutions operating in interstate commerce has a direct effect on interstate commerce; and

(5) the prosecution of persons engaged in computer-related crime is difficult under current Federal criminal statutes.

Id. § 2.

5. These losses are estimated at $90 billion annually. *Hearings, supra* note 2, at 118 (statement of E. J. Criscuoli, Jr.).

6. *See* note 28 *infra* and accompanying text.

7. *See, e.g., Computer Experts Accused of Theft of $10.2 Million to Buy Diamonds*, N.Y. Times, Nov. 7, 1978, at 1, col. 1.

8. The Security Pacific Bank theft did not involve computers. The culprit, Stanley Mark Rifkin, obtained the bank's password by observing the teletype operators in

a "computer" crime;[9] again, they were not.[10] The Equity Funding fraud,[11] one of the largest frauds ever committed, was also cited as a "computer" crime;[12] this claim has been much disputed.[13]

From information supplied by many federal government investigative agencies, the Government Accounting Office ("GAO") has reported a total of sixty-nine cases of "computer" crime in the entire federal government.[14] Actually, there were only sixty-six reported cases, since the Air Force erroneously identified three cases as computer crimes that did not even involve computers.[15] Nine of these cases involved no dollar loss, being incidents such as privacy invasion.[16] The total reported losses were $2,161,413;[17] the average loss was $44,000, and the median loss was $6,749.[18]

---

the transfer cage—a place to which he should not have been given access. He then telephoned the bank and, by impersonating a bank officer and supplying the correct password, was able to transfer funds from the Security Pacific Bank to a bank in New York. Amusingly enough, Rifkin used the wrong Security Pacific Bank number on his first attempt; he then obtained the correct account number from bank officials and repeated the phone call, this time successfully. Oddly, Donn Parker classifies this case as "computer abuse," because the transfer cage was located in the computer room. Personal communication between John K. Taber and Donn B. Parker.

9. *Hearings, supra* note 2, at 2 (statement of Sen. Joseph R. Biden, Jr.); *id.* at 18 (statement of Sen. Charles H. Percy).

10. The boxcar thefts resulted solely from the manipulation of manual records. Personal communications between John K. Taber and Donn B. Parker.

11. *See generally* D. PARKER, CRIME BY COMPUTER 118-74 (1976); R. SOBLE & R. DALLOS, THE IMPOSSIBLE DREAM. THE EQUITY FUNDING STORY: THE FRAUD OF THE CENTURY (1975).

12. *Hearings, supra* note 2, at 2 (statement of Sen. Joseph R. Biden, Jr.); *id.* at 18 (statement of Sen. Charles H. Percy); *id.* at 28 (statement of John C. Keeney, Deputy Ass't Atty. Gen., Crim. Div., Dep't of Justice).

13. R. LOEFFLER, REPORT OF THE TRUSTEE OF EQUITY FUNDING CORP. OF AMERICA, Oct. 31, 1974. *See also Hearings, supra* note 2, at 57 (statement of Donn B. Parker).

14. GAO REPORT, *reprinted in* SENATE COMM. ON GOV'T OPERATIONS, PROBLEMS ASSOCIATED WITH COMPUTER TECHNOLOGY IN FEDERAL PROGRAMS AND PRIVATE INDUSTRY, 95th Cong., 2d Sess. 71-91 (Comm. Print 1976) [hereinafter cited as GAO REPORT].

15. The correction to the GAO REPORT is from a statement by Joseph P. Welsch, Deputy Ass't Sec. of Defense for Management Sys. (Dec. 3, 1976), *reprinted in* SENATE COMM. ON GOV'T OPERATIONS, STAFF STUDY OF COMPUTER SECURITY IN FEDERAL PROGRAMS, 95th Cong., 1st Sess. 149 (1977) [hereinafter cited as COMPUTER SECURITY STUDY]. He also mentions that one Army case out of the sixteen involved conflict of interest on the part of computer management personnel rather than computer crime. *Id.* It is not clear, however, whether this case was included in the GAO study or not. Presumably, it was.

16. GAO REPORT, *supra* note 14, at 91, note c to table.

17. *Id.* at 91.

18. While the GAO REPORT did not supply the median, it is a simple matter to compute it from the tables. *Id.* at 90-91. Because of the distribution of data, the median is mathematically more meaningful than the average.

In a study[19] conducted by the Stanford Research Institute ("SRI"), based largely upon newspaper articles, the dollar loss for 1975[20] was given as $1.45 million.[21] This figure included the private sector as well as local and federal government.[22] The total accumulated loss for the past fifteen years has been given as $280 million;[23] with an average loss of $450,000 per case.[24]

Estimated annual losses, made by SRI and others, vary widely: $100 million,[25] $300 million,[26] and $160 million by 1985.[27] In contrast, the estimated losses from white collar crime in 1974 alone was $40 billion.[28]

These "computer crime" loss figures are very questionable. There is something particularly suspect about the average loss figure of $450,000, which is more than ten times the GAO average. It is probable that the difference is due to the fact that the SRI study was based upon the amount quoted in newspaper articles. Also, the actual losses for 1975 of $1.45 million is inconsistent with the claimed losses of $280 million over a fifteen year period—an amount two hundred times as great. This enormous discrepancy implies that computer crime is rapidly vanishing, or that the years 1976-1978 were incredibly lucrative years for computer criminals, or that 1975 was abnormally bad for these same persons.

SRI attributes this discrepancy to a time lag between the occurrence of a crime and its reporting.[29] This is a valid point, but not sufficient to explain the enormity of the discrepancy.[30] From the appearance of SRI's loss graph,[31] allowing for a time lag, and averaging the losses over the years, a reasonable loss for 1975 should be in the

---

19. D. PARKER, COMPUTER ABUSE ASSESSMENT (Stanford Res. Inst. Rep. 1975) [hereinafter cited as ASSESSMENT].

20. This is the most recent year for which complete figures are available.

21. ASSESSMENT, *supra* note 19, at 14 (Fig. 2).

22. *Id.*

23. *Hearings, supra* note 2, at 57 (statement of Donn B. Parker).

24. *Id.* at 18.

25. U.S. CHAMBER OF COMMERCE, A HANDBOOK ON WHITE COLLAR CRIME 4-6 (1974).

26. *Computer Capers*, TIME, Aug. 8, 1977, at 53. This figure was probably derived from PARKER, *supra* note 11, at 29-30. This figure is based upon the unjustified assumptions that one hundred cases will be reported each year, and that these reported cases constitute fifteen per cent of all computer-related crimes per year with an average loss of $450,000 per case. *Id.*

27. INSTITUTE FOR THE FUTURE, THE NATURE OF ECONOMIC LOSSES ARISING FROM COMPUTER-BASED SYSTEMS IN THE NEXT FIFTEEN YEARS (1972).

28. U.S. CHAMBER OF COMMERCE, *supra* note 25, at 5-9.

29. *Assessment, supra* note 19, at 12.

30. *Id.* at 14.

31. *Id.* at 12.

range of six to fifteen million dollars. But the loss curve is not well behaved; losses by years are fat or lean, and for 1976 through mid-1978, fantastic. The following table transcribes SRI's graph and shows yearly accumulated losses with yearly accumulated averages.

YEARLY LOSSES[32]

YEARS	YEAR	LOSS	ACCUMULATED LOSS	ACCUMULATED AVERAGE
1	1963	2.0	2.0	2.0
2	1964	5.1	7.1	3.55
3	1965	0.176	7.276	2.425
4	1966	0.0003	7.2763	1.819
5	1967	0.001	7.2773	1.455
6	1968	4.47	11.7473	1.9579
7	1969	2.002	13.7493	1.964
8	1970	11.6	25.3493	3.1687
9	1971	7.82	33.1693	3.685
10	1972	14.64	47.8093	4.7809
11	1973	8.74	56.5493	5.1408
12	1974	6.21	62.7593	5.2299
13	1975	1.45	64.2093	4.939
14	1976	not available	not available	
15	1977	not available	not available	
15.5	mid-1978		280.0	18.0645

A time lag cannot explain the minuscule loss of $300 in 1966. Nor can it explain the jump from a $64 million accumulated loss in 1975 to $280 million in mid-1978, just 2 1/2 years later. In plain English, these figures are too queer to be real! Far from being frightened by them as the proponents of S. 240 seem to be, one should question the data upon which these figures are based. SRI's data is unreliable and replete with unknown biases, as SRI is careful to point out.[33]

The author has personally examined more than seventy of SRI's "raw" cases—Cases 7711-74802, inclusive—the latest acquired by SRI at that time. These cases are not included in SRI's published totals, except perhaps in the mid-1978 figure of $280 million, but they do not differ in quality from cases described in the published reports. With few exceptions, the data available are newspaper clippings, mostly provided by clipping services. The obvious biases that appear in these cases include:

—the reporting of crimes that do not involve computers. These in-

32. *Id.* from figure at 14. Losses are given in millions of dollars.

33. *Assessment, supra* note 19, at 10 & 18. PARKER, *supra* note 11, at 25: ". . . public media are the predominant source . . . Newspaper accounts . . . are treated with particular skepticism." Unfortunately, skepticism or not, these newspaper cases are not excluded and account for many of SRI's cases and loss figures.

clude Fednet frauds, bank embezzlements, automatic teller machine frauds, and credit card frauds. The Stanley Mark Rifkin case,[34] by the way, was a Fednet fraud and the second such case to be misrepresented as a computer crime. The first one involved a different branch of the same bank and a Bausch and Lomb account in Illinois.[35]

—the reporting of crimes that are simply record manipulations, such as false invoices, false payments, and false billings. In these cases, while the records and office procedures are computerized, the computer is not manipulated to carry out the crime. For example, a stock broker employee, devoid of all technology, gives a data entry clerk a false margin for an account, and then borrows fraudulently against that account.[36]

—the reporting of crimes only if they are in some sense "newsworthy." In practice, this means that the amount of loss is extraordinary. The typical crime, the small crime, is simply never reported.[37]

—gross exaggerations of the amount lost, and distortions of the facts of the case, literally beyond recognition. In one case at Ames Research Center (SRI Case 77409), two "computer experts" were reported to have stolen time on the ILLIAC valued at "billions," based on an estimated rate of $100 a millisecond for ILLIAC time.[38] This story caused much mirth among computer

---

34. *See* note 8 *supra*.

35. SRI Case 78308. *See Ex-Controller Admits Guilt in $140,000 Fedwire Theft*, Computerworld, Aug. 14, 1978, at 1, col. 3. *See also Fed Moves to Tighten Security of Net As Potential for Transfer Loss Rises*, Am. Banker, May 25, 1978, at 1, col. 2. There may have been other, earlier cases that were not tagged "computer crimes" by the media.

36. SRI Case 77331. *See* Delsohn, *Tooley Hits Slap-on-the-Wrist Sentence*, Rocky Mtn. News, July 20, 1978; Seldner, *Brokerage Embezzler Receives Suspended Sentences*, Denver Post, July 20, 1978. *See also* Criminal Action No. 122398, City and County of Denver, State of Colorado, Arrest Warrant and Supporting Affidavit, which details the crime.

> The first two purchases of Loren Industries stock in the Robert Miller account were fraudulently switched to a "margin" account by altering the last two digits in the account number on the customer buy form. For all purchases of this stock thereafter, fraudulent transfer from a "cash" account to a "margin" account was accomplished by some person with access to the corporate records, making adjustment entries in accounting input records fed to the computer. These entries are handwritten on forms provided for the purpose.

Id. ¶ 11. Paragraphs 6, 7, and 8 detail what the "adjustment entries" were. Essentially they involved changing the cash account code associated with the account number to a margin account code, and changing the stock identification code to that of a legitimate margin stock code. All of this was manual paperwork. Incredibly, this was touted by the prosecutor as a computer crime, and carried as such by the media.

37. The "typical" crime involves about $6,700. GAO REPORT, *supra* note 14.

38. *See Case of the Stolen Time*, S. F. Chronicle, Jan. 21, 1978; and United Press Int'l, Press Release A236, 01-21 04:15 PES, and A061, 01-21 05:04 RES.

> scientists in the Bay Area. First, the rate of $100 a millisecond is almost twice the Gross National Product. Second, the ILLIAC wasn't involved, it was a much smaller PDP-10. Third, the "computer experts" weren't—one was a terminal repairman and the other a maintenance technician. The value later reported was less than $2,000 and it is more likely that the amount was a few hundred dollars. Actually the real crime was the physical theft of electronic equipment—the thieves used the PDP-10 to inventory their stolen goods.

Of course, there are clearly valid instances of computer crime in the SRI collection. The Flagler Dog Track trifecta fraud being the sharpest example (SRI Case 77322).[39] But these are few, though it is impossible to say how many without a thorough examination of all of the cases and a good definition of "computer crime."

The truth is, the SRI figures have no statistical validity.[40] SRI says that they have validity only as a "lower bound" of a still largely unexplored problem.[41] That is doubtful. The figures are not any

---

39. Details of the crime are contained in MALONEY, REPORT ON INVESTIGATING THE "SKIMMING" AT FLAGLER DOG TRACK (1977). Flagler Dog Track in Florida used two duplicate PDP-8 computers to compute the odds and payoffs in trifecta betting. Because the betting was fast and furious, and the computations were time-consuming—even for a computer—the dog race was often over before the computers finished their calculations.

A confederate communicated the results of the race to the computer room, where the computer operator threw the stop switch on one of the PDP-8s, causing the program to halt execution. At the console, the operator then "deducted" a number from the count of losers in computer storage, and added that same number to the count of winners, also in storage. He then restarted the computer and allowed the program to complete its computations. Later, the gang ran the ticket printers to print up fraudulent winning tickets, which other confederates cashed the next day. Since winners are paid from a pool formed by the losers' money, dog track officials would not detect the loss—each true winner would get a little less than he should.

The duplicate PDP-8 was intended to prevent such frauds. The gang, however, turned in a doctored report to track officials, and disposed of the incriminating report produced by the untampered second computer. In the opinion of the investigators, the crime could not have succeeded without lax auditing.

This is the only case the author has yet encountered that is indisputably a "computer" crime. It is amazing that phoney cases are touted by the proponents of S. 240, while this real one is treated with stentorian silence.

40. SRI admits as much:

> The 670 reported cases of computer abuse in our research at SRI International is not a statistical sample from which we can deduce how much crime associated with computers there may be. It represents a biased, incomplete collection of cases.

Testimony of Donn B. Parker before the State of California Senate Judiciary Committee regarding S.B. 66, May 1, 1979.

41. *Id.* ("It [the SRI cases] is merely a lower bound of incidence and loss that shows the existence and nature of a problem but does not tell us the size or seriousness of it.")

sort of a bound, lower or upper; rather, they are a point in a plane of unknown coordinates, meaningless until the cases are purged and purified. Yet, even were these figures blindly accepted, the fact remains that computer crime losses are insignificant when compared to white collar crime.[42]

Furthermore, the incidence rate of computer crime is also insignificant. Between the invention of the computer and 1975, there were 381 known incidents of computer "abuse" worldwide.[43] Of these cases, 77 were verified, 218 were assigned various "levels of confidence" (*i.e.*, probability that they actually occurred), and 86 were unverified.[44] Some of these cases are believed to be fictitious, and this is a very important point! Many well-known cases of computer crime, which have become part of the folklore, never occurred. They are totally mythical, yet computer professionals, law enforcement officers, politicians, and even researchers, widely believe and cite them.[45]

Even verification has its dangers. Donn Parker, a recognized expert in the field of computer abuse, reports that two cases which were verified turned out to be fictitious.[46] In other words, the figure of 381 "abuses," as small as it is, could very well be smaller, and

---

42. U. S. CHAMBER OF COMMERCE, *supra* note 25, at 5-9.

43. ASSESSMENT, *supra* note 19, at 6.

44. *Id.* at 10.

45. The "round-off" fraud is one example. In this fraud, the programmer accumulates the remainders after round-off in his account, instead of distributing them among all accounts. *See* PARKER, *supra* note 11, at 114-17. If there are many accounts over a period of time this fraud could result in a tidy sum. The possibility of fraud in round-offs, however, was well known long before computers were used, and is so well guarded against, that it was, and is, practically impossible to successfully perform. *Id.* at 117.

Another example is the Zwana/Zzwicke story, where the programmer short changes accounts and deposits the amounts in a false, last account. In one version of the story—SRI Case 71319N (D. PARKER, S. NYCUM & S. OURA, COMPUTER ABUSE, app., at 102 (Stanford Res. Inst. Rep. 1973)), the false account was a commission account for a fictitious salesman named Zwana. In another version of the story, the false account was for a customer named Zzwicke (reported with a straight face in Allen, *Embezzler's Guide to the Computer*, 53 HARV. BUS. REV., Jul.-Aug. 1975, at 87). In all versions of the story, the fraud is discovered when the marketing department of the company pulls the first and last names for a promotional campaign. The provenance of the story is a second generation computer that used punched card and tape files—that is why the false account is last.

The author strongly suspects that the MICR stories in the SRI cases (listed in COMPUTER ABUSE, *supra*, app., at 91, Cases 6431N, 6432N & 6433N), and by proponents of S. 240 (*see, e.g., Hearings, supra* note 2, at 13 (statement of Sen. Abraham Ribicoff); COMPUTER SECURITY STUDY, *supra* note 15, at 226) are also myths. There are many such myths, too numerous to mention.

46. ASSESSMENT, *supra* note 19, at 12.

must be treated with circumspection. Even accepting this figure for the purpose of this discussion, it leads to an "abuse" incidence rate of one case per year for every two thousand computers[47]—a very insignificant rate.

It must also be pointed out that not all of these 381 cases are criminal in nature. They include a large number of questionable uses of computers, as well as "odd" incidents.[48] Some do not even involve computers.[49] Of these cases, 145 involve fraud or theft.[50] A surprising number—sixty-six[51]—involve physical assaults on a computer, including four cases of a computer being shot, and one of a woman in France who beat a CRT terminal with her high-heeled shoe.[52] Many other cases involve only unethical, and not criminal, conduct. A good example is that of an instructor who used his school's computer to print fifty copies of campaign material for an election involving school issues.[53] Others involve student shenanigans with school computers, which usually did not involve criminal motives.

Because of loose definitions and somewhat arbitrary classifications,[54] it is difficult to determine the number of real crimes out of the 381 "abuse" cases. A good estimate is about 210 real criminal matters. These include false entry of records, fraud and embezzlement, theft—including the theft of computer programs and the theft of records—vandalism and sabotage. Yet, these are crimes that are already adequately covered by existing state and federal laws.[55]

---

47. *Id.*

48. *See, e.g.,* COMPUTER ABUSE, *supra* note 45, app., Case 6921N, at 93.

49. *See, e.g., id.*, Cases 7021N, 7111N & 71210Y, at 95, 97 & 99.

50. ASSESSMENT, *supra* note 19, at 30 (Table 6).

51. *Id.*

52. PARKER, *supra* note 11, at 18. *See also* COMPUTER ABUSE, *supra* note 45, app., Cases 6811N, 8213N, at 92, 104.

53. D. PARKER, COMPUTER ABUSE PERPETRATORS AND VULNERABILITIES OF COMPUTER SYSTEMS 24 (Case 7544) (Stanford Res. Inst. Rep. 1975). A similar case involving a student campaign is recounted *id.* at 21 (Case 72410).

54. "Stealing" a password is defined as theft.

55. Applicable federal laws are listed in COMPUTER SECURITY STUDY, *supra* note 15, at 210-22. There is a legal nicety involved in the theft of programs and computerized records. Generally, the theft does not involve asportation, *i.e.*, there is no "taking" in the legal sense, since the owner is not deprived of the program by the theft. *Hearings, supra* note 2, at 123 (letter from E. J. Criscuoli, Jr.). Instead, the theft involves a wrongful copying. Thus the thief cannot be charged with larceny (common law theft), but must be charged instead with a theft of trade secrets or a copyright violation (statutory charges). There are some who feel that the law should be modified to support common law theft charges in these cases. It is a minor issue; it makes little difference whether the thief is punished for larceny-type theft or a trade secret theft. *See also* Nycum, *The Criminal Law Aspects of Computer Abuses*, 5 RUTGERS J.

There are over forty applicable laws at the federal level alone.[56] S. 240 is simply not necessary.

There are other "estimates" that should also be mentioned. One is that only one-fifth of detected "computer" crimes are reported to the authorities from fear of embarrassment.[57] There is no evidence to support this contention. Furthermore, federal regulations require financial institutions to report all crimes.[58] It seems unlikely that they fail to do so, unless there has been a massive breakdown in the enforcement of banking regulations. If there has been, a new law will hardly cure the problem. Another estimate is that only one-hundredth of all "computer" crimes are ever discovered.[59] There is no evidence to support this estimate either.

It is claimed that the use of the computer for fraud creates a unique sort of crime that requires it own criminal law.[60] This is doubtful. The use of a computer to perpetrate a fraud is equivalent to the use of an office adding maching or tub file. It is inconceivable that a federal law is needed to cover the case of a computer operator who, in frustration, shoots his computer, or the woman who attacks her terminal.

There is an ancient principle that holds that the law is concerned with serious matters, not with trivia. The appropriate sanction for cases like that of the instructor who misuses the school computer is a reprimand from his employer, or even dismissal, but certainly not fifteen years in federal prison. The system programmer who, without authorization, plays tic-tac-toe on a computer should be beneath notice of the law.

It is argued that computer crimes are difficult to prosecute.[61] Quite the contrary, convictions for crimes involving computers have been easy to obtain, sometimes with federal prosecutors intruding into the sphere of state sovereignty. In the Kelly and Palmer case in

---

COMPUTERS & L. 271 (1976); Nycum, *Legal Problems of Computer Abuse, reprinted in Hearings, supra* note 2, at 173, 174 n.3, & 175 nn.5, 7.

56. *Id.* at 3, 36 (statement of Sen. Joseph R. Biden, Jr.); *id.* at 71, 72 (statement of Susan H. Nycum).

57. This figure was quoted skeptically by Senator Biden. *Id.* at 37.

58. ASSESSMENT, *supra* note 19, at 26.

59. A. BEQUAI, COMPUTER CRIME 4-6 (1978). This figure is attributed elsewhere to the Commerce Department. *Hearings, supra* note 2, at 18 (statement of Sen. Charles H. Percy). Bequai, adjunct professor of law at American University, is the principal author of S. 240, along with Phil Manuel of the Senate Government Affairs Committee staff.

60. *Hearings, supra* note 2, at 34-35 (statement of Joseph E. Henehan, Chief, White Collar Crime Div., Dep't of Justice).

61. *See, e.g., id.* at 11 (statement of Sen. Abraham Ribicoff).

Philadelphia,[62] the defendants used their employer's computer without permission for their own outside music business. The federal prosecutor charged them with mail fraud for advertising their music, and the defendants were convicted. This is a clear case of unwarranted federal intrusion into a state matter.[63]

The United States attorney complained at the hearings on the Ribicoff bill that the judge in *United States v. Jones*[64] would not allow a charge of interstate transportation of fraudulently obtained securities—a decision which he attributed to the legal complexities caused by computers.[65] In *Jones*, Michael Everston provided false records to a Canadian corporation's computerized record system, causing the computer to print checks payable to Everston's sister, Amy Everston Jones, in Maryland. The prosecutor charged Jones with interstate transportation of fraudulently obtained securities. The district judge, however, ruled that the indictment was invalid because the crime was actually forgery in a foreign country, over which the United States has no jurisdiction.[66] The question was not the complexities caused by computers, but one of jurisdiction: Did the crime fall to Canadian authorities to prosecute, Maryland authorities, or federal? The Fourth Circuit Court of Appeals reversed the trial judge, ruling that the checks were securities, not forgeries.[67] Jones was thereafter tried and convicted.[68] The "complexities" of this case were not due to the presence of a computer, but to the eagerness of the prosecutor where the jurisdiction of the United States was not immediately apparent.

This case has sparked surprising misinterpretations. A computer security professional, the same one who told the newspapers that ILLIAC charges should be $100 per millisecond, said in a panel discussion at the Third West Coast Computer Faire, that the district judge ruled that the computer committed the forgery but that there was no way to prosecute a computer. Senator Ribicoff cited this case as one which the government "lost."[69] Perhaps the real legal problems of computer crime are not the results of a supposed lack

62. *Computer Capers, supra* note 26, at 53.

63. The *Seidlitz* case (United States v. Seidlitz, 589 F. 2d 152 (4th Cir. 1978)), involving the theft of a computer program, is another intrusion into a state matter, though in *Seidlitz* the prosecutor claimed that the local police requested federal intervention. *Hearings, supra* note 2, at 88 (statement of Jervis Finney).

64. 414 F. Supp. 964 (D. Md. 1976), *rev'd*, 553 F. 2d 351 (4th Cir. 1977).

65. COMPUTER SECURITY STUDY, *supra* note 15, at 236-38. *See also Hearings, supra* note 2, at 88 (statement of Jervis Finney).

66. United States v. Jones, 414 F. Supp. 964, 969 (D. Md. 1976).

67. United States v. Jones, 553 F.2d 351, 356 (4th Cir. 1977).

68. *Hearings, supra* note 2, at 88 (statement of Jervis Finney).

69. 125 CONG. REC. 711 (daily ed. Jan. 25, 1979). Senator Ribicoff's assertion is sur-

of understanding of computers, but bungled indictments, improper prosecutions, and in general, a lack of understanding of the law. Blaming the computer is the traditional out for one's own errors. But, even so, in every known case in which a real crime occurred, the prosecutor has been able to secure a conviction under one or more existing laws.[70]

II. PRISON INMATE PROGRAMMING

The Department of Justice, and other proponents of S. 240, contend that computer crime is easy to commit and difficult to detect. For inexplicable reasons, they regard programmers with suspicion and hostility. The Federal Bureau of Investigation is afraid of "computer freaks,"[71] and a *Time* magazine article on computer crime, the obvious source of which was the Department of Justice, concluded with the statement that "[i]deally, the first step in securing a system would be to shoot the programmer."[72]

This hostility is impossible to understand. Studies of computer crime, as flawed as they are, all agree that programmers are seldom the perpetrators of computer crimes. The culprit is usually the data entry clerk or manager. Yet, paradoxically, this fear and hostility towards programmers in general does not seem to apply if the programmers are armed robbers, murderers, or forgers. The Department of Justice's Bureau of Prisons currently operates a small, but burgeoning, data processing service employing convicts in at least six federal prisons.[73] Customers for these services have included the Department of Defense, Department of Agriculture, Internal Revenue Service, the Bureau of Prisons itself, Department of Commerce and General Services Administration.[74] The Department of Agriculture has even located its new computer center in Kansas

---

prising, coming six months after the prosecutor, testifying on the Senator's own bill, announced with pleasure the reversal of the district judge's ruling.

70. Personal communication between John K. Taber and Donn B. Parker.

71. COMPUTER SECURITY STUDY, *supra* note 15, at 243.

72. *Computer Capers, supra* note 26, at 53.

73. In fiscal year 1976, the prisons providing these services were Alderson, West Virginia; Lexington, Kentucky; Miami, Florida; Terminal Island, California; Fort Worth, Texas; and Leavenworth, Kansas. FEDERAL PRISON INDUS., INC. (UNICOR), ANNUAL REPORT 16 (1978). At the present time, there are probably state prisons providing contract data processing services. Minnesota had a bill in Congress to allow interstate commerce of prisoner written computer programs. *See Hearings on Job Training Before the House Educ. and Labor Comm.*, 94th Cong., 2d Sess. (1976). *See also* COMPUTER SECURITY STUDY, *supra* note 15, at 73-123.

74. FEDERAL PRISON INDUS., INC. (UNICOR), ANNUAL REPORT 9 (1978); COMPUTER SECURITY STUDY, *supra* note 15, at 84.

City, Missouri, just to be close to the convict programmers located in Leavenworth Federal Penitentiary.

The gross earnings from these services in fiscal year 1977 were just under one million dollars.[75] Data entry services are also provided for the Navy by female offenders in Alderson, West Virginia, and Terminal Island, California.[76] Programming is provided by Leavenworth inmates for the Agricultural Stabilization and Conservation Service of the Department of Agriculture.[77] These programs form part of the general ledger and accounting programs of the Department of Agriculture, and affect the disbursement of funds.[78] The same Leavenworth inmates have reportedly written unspecified programs for the Internal Revenue Service.[79] Indeed, there were rumors at one time, apparently unfounded, that the convicts learned enough about the IRS computerized tax return system to enable them to file fraudulent returns that escaped detection by the IRS.[80]

Future prison data processing business can only grow, if enough prisoners can be found who are willing and able to write programs. The General Services Administration, no doubt at the urging of the Department of Justice, has promulgated Federal Procurement Regulation 1-5.402.[81] This regulation requires all federal agencies to give priority to the Federal Prison Industries, Inc. over private industry for all data entry and programming services. The affected agencies are required to pay the current commercial rate for these services, with perhaps a small incentive deduction.

There is clearly something wrong. On one hand, the Department of Justice is asking for broad, dangerous, statutory powers, claiming that computer crime is so easy to commit and so difficult to detect; on the other hand, the same agency apparently sees nothing wrong with prisoners convicted of serious crimes programming sensitive accounting applications. Indeed, the Department is even attempting to increase such activities through federal regulation.

---

75. FEDERAL PRISON INDUS., INC. (UNICOR), ANNUAL REPORT 9 (1977). The areas of data processing and printing were consolidated in the 1978 Annual Report, so it is impossible to determine how much was earned by data processing services alone.

76. FEDERAL PRISON INDUS., INC. (UNICOR), ANNUAL REPORT 6 (1978).

77. COMPUTER SECURITY STUDY, *supra* note 15, at 99-108; 123 CONG. REC. 17067 (daily ed. Oct. 12, 1977) (statement of Sen. Abraham Ribicoff), *reprinted in Hearings, supra* note 2, at 184.

78. *Id.*

79. *Id.*

80. *Id.* at 13-14 (statement of Sen. Abraham Ribicoff); 123 CONG. REC. 17,067-68 (daily ed. Oct. 12, 1977) (statement of Sen. Abraham Ribicoff), *reprinted in Hearings, supra* note 2, at 184. *See also* COMPUTER SECURITY STUDY, *supra* note 15, at 76-77, 88-89, 91-98 & 108-15.

81. *Id.* at 87.

The truth is—there is nothing wrong with prisoners writing programs. Computer crime is not easy to commit, and the Bureau of Prisons' program is living proof. This is the one good, job training program in the entire federal prison system. Qualified convicts are learning a useful trade, unlike the usual prison jobs, and are quickly hired on release for meaningful, well-paid jobs. As one would expect, the recidivism rate for convict programmers is extremely low.[82] The "bottom line" is that the Department of Justice is pursuing a schizophrenic course in supporting the Ribicoff bill.

III. This Bill Outlaws Common Practices

Section (b) of the bill is simply too broad. It fails, and in fact does not even attempt, to distinguish between felonious uses of computers, lesser criminal uses of computers, and ethically questionable or simple unauthorized uses. This failure threatens to make criminals out of a large portion of the computer profession.

"Unauthorized" use of computers is widespread among programmers.[83] Programmers on occasion use their employer's computer to play games like tic-tac-toe or Star Trek. They draw tabby cat calendars and pin-up girls. They have discovered that by using certain combinations of nonsense character combinations on IBM 1403 printers they can generate musical tones; there is at least one programmer who can play "She'll Be Comin' Round the Mountain" on the printer, with judiciously timed page ejects as a drum beat accompaniment.

Programmers' ingenuity is amazing. They use the computer to balance their checkbooks, chart the misfortunes of their stocks, and figure mortgage tables. They write "unauthorized" programs, out of curiosity, that have little earthly use, like the knight's tour of the chessboard, or a base-256 multiplier. Sometimes an "unauthorized" program proves useful and, through the programmers' "grapevine," becomes unofficially adopted at computer centers throughout the world. This play and incidental personal use is without pecuniary motive. Yet, all of it would be a federal offense under Section (b) of the Ribicoff bill.

There are some who argue that such play should be forbidden; that the computer is not a toy, but a very expensive asset; and, that such games steal time and resources from their rightful owners. This argument has merit, but S. 240 is a radical solution to the problem—if it is a problem. Imprisonment for fifteen years is a sanction

82. *Hearings, supra* note 2, at 63 (statement of Donn B. Parker); Computer Security Study, *supra* note 15, at 77-78.

83. *Id.* at 54 & 68.

totally out of proportion to the "offense." The bill is an improper intrusion into an area where there is no legitimate public policy interest. Employment sanctions have been, and should continue to be, the adequate and proper remedy.

Employer's views on "unauthorized" uses vary widely. Some flatly forbid any non-business uses of their computers, and police machine usage to enforce the ban. Others forbid the practice in theory, but allow it in practice, and even "wink" at it. Still others permit it as a fringe benefit of employment.[84] For many companies, such use has never been considered a "problem" that needed to be addressed.[85] Thus, an act committed on one computer might be perfectly legal, and even win the programmer a commendation, while the same act, performed on the same computer in another location, could cause his imprisonment. S. 240 could never be equitably enforced.

Great care must be exercised in forbidding such uses. Eliza, for example, can be considered a "game," yet is a classic in artificial intelligence research. Many "games," in fact, provide great insight into computer programming and are of professional benefit. In many areas of science, mathematics, and computer science it is impossible to distinguish between "unauthorized" uses and legitimate research. Researchers will find this bill an intolerable infringement on their creative freedom.

S. 240 does not address the problem of who may authorize what uses of the computer. Presumably, the authorizer is the employer. Yet, this leads to the absurd conclusion that the Equity Funding fraud would not have violated section (b), since the officers of the company authorized use of the computer in perpetrating the fraud.

Who may authorize what use is not an idle question. "Employers" are often simply users of computer equipment, and own neither the hardware nor the software. The owner-lessor does not relinquish his rights by renting these items to the user. Yet, it is common practice for the user to alter rented code, and even hardware, without express authorizaton from the owner. Section (b), which makes unauthorized alteration of computer programs a felony, will

84. *Id.* at 80 (statement of Robert P. Abbott).

85. *Id.* at 54 (statement of Donn B. Parker). IBM prohibits non-business uses of their computers, and conducts internal audits to ensure compliance. If Hewlett-Packard has a similar ban, their programmers are unaware of it. Many smaller firms, too numerous to mention, allow non-business uses as a fringe benefit. An example of an unofficial program is DEBE (*D*oes *E*verything *B*ut *E*at). It is a useful utility program, written without specific authorization, and in use wherever there are IBM computers. There are many other programs like DEBE. *See also id.* at 150-51 (statement of Peter S. Browne).

force wholesale renegotiations of software, and to a lesser extent hardware, leasing contracts. There is no compelling reason to change this common industry-wide practice.

IV. The Bill Makes Felonies Out of Absurdities

The definition of a "computer" contained in S. 240 is too broad: " '[c]omputer' means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses. . . ."[86] This definition would include, and is apparently meant to include, pocket calculators, and even some digital watches.[87] Microprocessors enjoy wide application today in all sorts of gadgets. Under this bill, a secretary who uses an automatic typewriter to type a personal letter, or the office worker who uses his company's calculator to balance his checkbook, is a felon. It is doubtful that this definitional problem can be overcome, since the industry itself has never been able to agree on a generally accepted definition of "computer" for technical purposes, let alone legal.[88]

V. The Bill May Be Abused

This bill has a dangerous potential for abuse. First, it is a seri-

---

86. S. 240, 96th Cong., 1st Sess. § 3(a)(2) (1979).

87. When it was pointed out to the staff members of the Government Affairs Committee, who helped draft this bill, that their definition of computer included trivia like pocket calculators, they indicated that they meant to do so. They posited a bizarre illustration of a mortgage applicant tampering with a bank officer's calculator to make the payments fraudulently benefit the applicant. Private communication between John K. Taber and Donn B. Parker. *See also Hearings, supra* note 2, at 67 (statement of Donn B. Parker).

88. Donn Parker attempted to get several computer scientists to define "computer" for California Senate Bill S.B. 66, State Senator Lou Cusanovich's "little Ribicoff bill," introduced in December 1978. The text of the current version of S.B. 66 is set forth in the Appendix to this article. Agreement, however, has been difficult to achieve. The problem is to exclude trivia like calculators at one end of the scale, and the telephone system, which is the largest special purpose computer ever built, at the other. The purpose of such an exercise is to limit the definition of "computer" to a general purpose digital computer used for record keeping. Eventually, Parker did get a definition, which had to be rejected for being too complex and technical for a lay jury to understand. Private communications between John K. Taber and Charles Mobley, Senator Cusanovich's staff consultant. *See also* Gruenberger, *What's in a Name?*, 25 DATAMATION, May 1979, at 230:

> It is discouraging we can't, as a profession, get simple things like definitions straight. Perhaps we will never be able to fabricate a decent definition of a term like "systems analyst," but we ought to be able to pinpoint a term like "computer." If we don't, then some ill-informed judge will pinpoint them for us, and we won't like the outcome.

ous threat to privacy. Second, there is an obvious danger of imprisoning programmers and other computer users for mere bagatelles.

From society's point of view, record-keeping is the most important use of computers today. Most record-keeping is computerized, and virtually all records soon will be. This bill, since it is so broad, gives the FBI, under its investigative powers, a right of access to records to which it never before had access. This point was made by Senator Biden at the hearings on S. 240:

> I know that there is a good deal of criticism and concern about abuse of power by [the FBI, the CIA, and our security industry].
>
> We are going to be turning to these agencies and saying "We are going to broaden your jurisdiction now. We are going to allow you legally to get into a number of data banks that you did not have access to before." * * * [Y]our legislation is very broad. As I read it, just about any computer in America will be accessible for the first time to investigation by a major Federal law enforcement agency.[89]

The point is undeniable, and Senator Charles Percy, to whom Senator Biden addressed these remarks, did not deny it.[90] Senator Percy allowed that S. 240 was not a panacea[91] and, when Biden pressed the point, Percy expressed pious hopes that a privacy bill, "vitally needed" but not yet enacted, would help prevent abuses.[92]

The second potential abuse is the arbitrary jailing of programmers for slight indiscretions. As has already been noted,[93] "unauthorized" use of computers is widespread. The bill will not change that fact. Most programmers and other users will remain unaware of the law. Further, whether or not correct, programmers do not feel that their personal use of computers is wrong, as long as it is not for material gain.

Third, even if some become aware of the law, they will not believe that it applies to their "unauthorized" use of computers. Generally speaking, computer professionals are technically-oriented and do not know or care about laws. The result will be that most programmers and other computer users will be unprosecuted felons, vulnerable to the charging abuses of overzealous prosecutors.[94]

This bill gives too much discretionary power to law enforcement

89. *Hearings, supra* note 2, at 24-25 (statement of Sen. Joseph R. Biden, Jr.).

90. *Id.* at 25.

91. "I am not saying this is a panacea, but this is the quickest way. We do not want to make it a complicated bill." *Id.*

92. *Id.* Nor did Senator Ribicoff, the Department of Justice or the FBI deny the point.

93. *See* note 83-85 *supra* and accompanying text.

94. *Hearings, supra* note 2, at 68 (statement of Donn B. Parker).

officers. While some discretion is necessary for effective law enforcement, modern American history does not make happy reading in the enforcement of broad statutes. The FBI has abused its powers; it has acted illegally in searches and seizures. Why encourage further abuses?

Would this law be abused? The Department of Justice says that it would prosecute only those cases in which the federal government has a "compelling interest."[95] This is cold comfort. It means that if a programmer is jailed for playing computer tic-tac-toe, it must be presumed that the government had a compelling interest. Nowhere does either the FBI or the Department of Justice explicitly promise not to prosecute a programmer who plays tic-tac-toe or draws a calendar, even under direct questioning on the point:

> BIDEN: * * * Let us level with the public. Let us acknowledge to them, by implication at least, that we are not going to prosecute that particular person. . . .
>
> FINNEY (Department of Justice): The Snoopy [calendar] was our case.
>
> BIDEN: Yes. Acknowledge that we are not going to prosecute Snoopy and do not leave the possibility of abuse, which does exist now.[96]

Finney's response covers several pages, mentions the good sense of the FBI and the Department of Justice, and claims that trust is needed.[97] Yet, nowhere does he give the acknowledgement requested. He purposefully avoids committing the Department of Justice not to prosecute such activities.

Will computer users be jailed for these trifles? The probability is grim. Past performance is one indication, but even more important is impetus. Computer crime does not exist; it is a misnomer applied to several crimes that may or may not involve computers—generally, record-keeping crimes. But it is a new, glamorous crime sensationalized by the media. Even Dick Tracy is fighting computer

---

95. *Id.* at 36 (statement of John C. Kenney, Deputy Ass't Atty. Gen., Crim. Div., Dep't of Justice).

96. *Id.* at 91 (statement of Jervis Finney). The choice of Snoopy calendars as the generic example for this type of "playing around" is due to Donn Parker of SRI, and is poorly chosen. Years ago, Charles Schulz' attorneys requested that the industry stop the making of Snoopy calendars, because the practice infringed on Mr. Schulz' copyrights. Management agreed, and suppressed the practice. The author has not personally seen an illicit Snoopy calendar since about 1970. All participants in discussions on the computer crime bill should refrain from using this example so as to avoid unnecessarily alarming Mr. Schulz. If a generic term is needed, such items as tic-tac-toe, or the contemporary rage "Adventure," written by computer scientists at MIT and Stanford's artificial intelligence laboratory, could be used.

97. *Id.*

crime.[98] Computer crime suffers from great publicity, which in turn creates the impression that it is a widespread problem. This publicity generates political pressure for the prosecution of computer crimes. Unfortunately, there are scarcely any such crimes, except the playing of tic-tac-toe. The prosecutor, trained for and assigned to prosecute computer crime, will have to be content with prosecuting this "criminal" plague if he expects to advance his career.

The reader may think it unlikely that a judge would permit prosecution of this type of activity. Unfortunately, a judge will have little choice. Senator Ribicoff, on reintroducing this legislation as S. 240, said that this type of "playing around" is the same type of activity that encourages computer crimes.[99] He cites as an example a Department of Agriculture employee at the Washington Computer Center who permitted his children to play games on the Department's computer. There is scarcely a programmer in the country who has not done the same. But the same employee also used the WCC computer for his own outside consulting business. The drift of Senator Ribicoff's contention is that the main purpose of the bill is not to jail programmers for "playing around," but that to change the language of the bill to accommodate "playing around" would seri-

98. Dick Tracy seems to be out-and-out Department of Justice propaganda. Richard L. Thornburgh, Assistant Attorney General said in 1976:

> Computer users are curiously ambivalent about security. Consider the business man who would never leave his checkbook lying on top of his desk . . . This same business man will purchase a multimillion dollar computer . . . without an audit as basic as a cancelled check—will place a computer terminal on the top of the desk unattended.

COMPUTER SECURITY STUDY, *supra* note 15, at 228. And this from Dick Tracy, Jan. 28, 1979:

> DETECTIVE SAM: Sir, do you leave your billfold out on your desk, when you go to lunch?
> WALTER PREMIUM (Business man, president of Equity America Life, whose computer is a "$1,000,000 loss" due to a shotgun fired in its chips, "not just the computer, but data too"): *What*? Certainly not!
> DETECTIVE SAM: Well, doesn't a multi-million dollar computer complex deserve as much consideration as a *billfold*? During the lunch hour here, only a secretary and a computer programmer stood between a MANIAC and your elaborate computer system.

Thornburgh, by the way, is now governor of Pennsylvania.

99. 125 CONG. REC. 719 (daily ed. Jan. 25, 1979). Throughout this lengthy debate Ribicoff stressed government computers, over which Congress, as an employer, may be presumed to have a rightful interest in their use for non-business purposes. Only at the end, in one brief clause, does he mention computers of "certain organizations involved in interstate commerce." *Id.* at 720. The impression created by his emphasis on federal computers is disingenuous. Senator Ribicoff is certainly aware that the bill covers computers of "entities affecting interstate commerce," meaning virtually all computers in the private sector, not just "certain" interstate organizations.

ously weaken it. If an innocent programmer runs afoul of the language, too bad; he should not be "playing around" anyway.

This is not just a Senator's overzealous advocacy. Trial judges, when attempting to apply new law in a doubtful case, consult the legislative record to determine the law's intent. Unless there are constitutional grounds, the judge is required to respect that intent. The Constitution does not forbid bad laws, only certain bad laws. Senator Ribicoff's comments were clearly an expression of legislative intent. If S. 240 becomes law, judges will feel compelled to permit trial of the tic-tac-toe'er, limiting the scope of trial to a factual determination of whether or not the tic-tac-toe player intentionally played without authorization. Though the programmer may not receive a stiff sentence, even the judge's discretion in this area may be seriously circumscribed. Senate Bill S. 1437[100] may soon become law. This bill limits the judge's sentencing discretion to a formula of plus or minus twenty-five percent. Under that law, a programmer's sentence would have to be between eleven years and nineteen years.[101]

For sometime now, the FBI has been training prosecutors and other law enforcement personnel on computer crime. The FBI conducts both a one week course and a four week course at Quantico, Virginia. The one week course has had over five hundred graduates. Mr. Henehan of the FBI said in testimony that " . . . there is a reluctance on the part of both the prosecutors and the investigators to get into these cases [that is, computer crime]. We find that through training they are much more anxious to accept a case."[102] This course apparently generates enthusiasm for prosecuting computer crimes.

The FBI also thinks that it will need two hundred more special agents, forty-five more accountant technicians, and ten auditor-computer specialists to fight computer crime.[103] What this means is that a large number of people are being trained to prosecute and investigate computer crimes. While this is a glamorous new area, there is currently little to do except prosecute programmers playing tic-tac-toe.

The chances for abuses from this legislation are enormous. The only protection to the public is the promise of the FBI and Department of Justice that we can trust their good sense.

---

100. *Hearings, supra* note 2, at 48-49 (statement of Sen. Joseph R. Biden, Jr.)

101. *Id.*

102. *Id.* at 35.

103. *Id.* at 110 (statement of John C. Keeney, Deputy Ass't Atty. Gen., Crim. Div., Dep't of Justice).

VI. CONCLUSION

Senate bill S. 240 is an ill-drafted and dangerous law that must be rejected. Minor flaws could be corrected, but the bill is fundamentally and fatally flawed. For example, one minor flaw is the incorrect use of the noun "access" as a verb for no apparent reason.[104] This usage is computer jargon that Congress should not enshrine in the United States Code. Section (a), which duplicates existing fraud laws,[105] should also be eliminated as unnecessary.

The fundamental flaw, however, is that the bill defines an abstraction—"computer crime"—as a crime, rather than proscribing specific acts. The phrase "computer crime" (or "filing cabinet crime") beclouds specific criminal acts, and non-criminal acts, with a trope drawn from the instrumentality of the acts. While it is true that one may commit murder with a filing cabinet by dropping it on the victim, and one may tamper with records by using a computer, nevertheless, the crimes are murder and fraud, not unauthorized use of a filing cabinet or unauthorized access to a computer.[106]

S. 240 is a bad bill, a dangerous bill, and should be opposed.

---

104. S. 240, 96th Cong., 1st Sess. § 3(c)(1) (1979).

105. 18 U.S.C. §§ 1341, 1343 (1976).

106. A computer is just a technique or method by which people are doing the same types of things that have been done in the past—embezzlement, thefts from their employers, and so forth. The computer merely gives certain people with knowledge and access an increased opportunity to do this sort of thing and in some situations the opportunity to do it in a greater way than it would be possible with the normal embezzlement and other criminal techniques.

Hearings, supra note 2, at 43 (statement of John C. Keeney, Deputy Ass't Atty. Gen., Crim. Div., Dep't of Justice).

APPENDIX

96TH CONGRESS
1ST SESSION

S.240

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

IN THE SENATE OF THE UNITED STATES

JANUARY 25 (legislative day, JANUARY 15), 1979

MR. RIBICOFF (for himself, Mr. PERCY, Mr. KENNEDY, Mr. INOUYE, Mr. JACKSON, Mr. MATSUNAGA, Mr. MOYNIHAN, Mr. WILLIAMS, Mr. ZORINSKY, Mr. DOMENICI, Mr. STEVENS, Mr. CHILES, and Mr. NUNN) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1979".

SEC. 2. The Congress finds that—

(1) computer-related crime is a growing problem in the Government and in the private sector;

(2) such crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;

(3) the opportunities for computer-related crimes in Federal programs, in financial institutions, and in other entities which operate in interstate commerce through the introduction

of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great;

(4) computer-related crime directed at institutions operating in interstate commerce has a direct effect on interstate commerce; and

(5) the prosecution of persons engaged in computer-related crime is difficult under current Federal criminal statutes.

SEC. 3.(a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

"§1028. Computer fraud and abuse

"(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 which, in whole or in part, operates in interstate commerce or is owned by, under contract to, or in conjunction with, any financial institution, the United States Government or any branch, department, or agency thereof, or any entity operating in or affecting interstate commerce, 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 false or fraudulent pretenses, representations or promises, shall be fined a sum not more than two and one-half times the amount of the fraud or theft, or imprisoned not more than fifteen years, or both.

"(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 described in subsection (a), or any computer software, program or data contained in such computer, computer system or computer network, shall be fined not more than $50,000 or imprisoned not more than fifteen years, or both.

"(c) For purposes of this section, the term—

"(1) 'access' means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network;

"(2) 'computer' means an electronic device which performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses, and includes all input, out-

put, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network;

"(3) 'computer system' means a set of related, connected or unconnected, computer equipment, devices, and software;

"(4) 'computer network' means the interconnection of communication systems with a computer through remote terminals, or a complex consisting of two or more interconnected computers;

"(5) 'property' includes, but is not limited to, financial instruments, information, including electronically processed or produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value;

"(6) 'services' includes, but is not limited to, computer time, data processing, and storage functions;

"(7) 'financial instrument' means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security, or any electronic data processing representation thereof;

"(8) 'computer program' means an instruction or statement or a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

"(9) 'computer software' means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system;

"(10) 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) a member of the Federal Reserve including any Federal Reserve bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank systems and any home loan bank;

"(F) a member or business insured by the Securities Investor Protection Corporation; and

"(G) a broker-dealer registered with the Securities and

Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934".

(c) The table of sections of chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following:

"1028. Computer fraud and abuse.".

AMENDED IN ASSEMBLY JUNE 19, 1979
AMENDED IN SENATE MAY 17, 1979
AMENDED IN SENATE MAY 9, 1979
AMENDED IN SENATE APRIL 23, 1979
AMENDED IN SENATE FEBRUARY 15, 1979

SENATE BILL **No. 66**

Introduced by Senator Cusanovich

December 5, 1978

An act to add Section 502 to the Penal Code, relating to computer crime.

LEGISLATIVE COUNSEL'S DIGEST

SB 66, as amended, Cusanovich. Computer crime.

Existing law relative to crimes involving fraud, or unauthorized access to, or damage or destruction of, property does not contain any specific provision relative to computers.

This bill would make it a crime, as specified, to intentionally access or cause to be accessed any computer system, or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property or services with false or fraudulent intent, representations, or promises; or to maliciously access, alter, delete, damage, or destroy any computer system, computer network, computer program, or data.

Under existing law, Sections 2231 and 2234 of the Revenue and Taxation Code require the state to reimburse local agencies and school districts for certain costs mandated by the state. Other provisions require the Department of Finance to review statutes disclaiming these costs and provide, in certain cases, for making claims to the State Board of Control for reimbursement.

This bill provides that no appropriation is made by this act pur-

suant to Section 2231 and 2234 for a specified reason, but recognizes that local agencies and school districts may pursue their other available remedies to seek reimbursement for these costs.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program. yes.

The people of the State of California do enact as follows:

SECTION 1. Section 502 is added to the Penal Code, to read:

502. (a) For purposes of this section:

(1) "Access" means to instruct, communicate with, store data in, or retrieve data from a computer system or computer network.

(2) "Computer system" means a machine or collection of machines, ~~used for governmental, educational, or commercial purposes~~, one or more of which contain computer programs and data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(3) "Computer network" means an interconnection of two or more computer systems.

(4) "Computer program" means an ordered set of instructions or statements, and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

(5) "Data" means a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network.

(6) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof.

(7) "Property" includes, but is not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.

(8) "Services" includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system, or data contained within a computer network.

(b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or ex-

tort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense.

(c) Any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.

(d) Any person who violates the provisions of subdivision (b) or (c) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

(e) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction.

SEC. 2. Notwithstanding Section 2231 or 2234 of the Revenue and Taxation Code, no appropriation is made by this act pursuant to these sections because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction. It is recognized, however, that a local agency or school district may pursue any remedies to obtain reimbursement available to it under Chapter 3 (commencing with Section 2201) of Part 4 of Division 1 of that code.