Washington and Lee Law Review

Volume 38 | Issue 4 Article 5

Fall 9-1-1981

# A Suggested Legislative Approach to the Problem of Computer Crime

# NOTES

## A SUGGESTED LEGISLATIVE APPROACH TO THE PROBLEM OF COMPUTER CRIME

Since the invention of the first computer in the 1950's,[1] computers have become an increasingly pervasive force in American society.[2] As the use of computers for legitimate purposes has increased, the involvement of computers in illegitimate activity has increased as well.[3] Unfortunately, the application of traditional legal theories[4] and law enforce-

---

[1] *See generally* J. SOMA, THE COMPUTER INDUSTRY 15-21 (1976) [hereinafter cited as SOMA]. Although a number of electronic calculating devices appeared during the 1940's, the machines operated without the benefit of stored programs. *Id.* at 16. Pioneers in the computer field completed the first machine to operate from an internally stored program in 1950. *Id.* The first commercially salable computer emerged in 1954. *Id.* at 17.

[2] *See* Swanson & Territo, *Computer Crime: Dimensions, Types, Causes, and Investigation*, 8 J. OF POLICE SCI. AND AD. 304 (1980) [hereinafter cited as Swanson & Territo]. *See generally Computer Systems Protection Act of 1979: Hearings on S. 240 Before the Subcomm. on Criminal Justice of the Senate Comm. on the Judiciary*, 96th Cong., 2d Sess. 26-38 (1980) [hereinafter cited as *1980 Hearings*] (statement of Michael Dertouzos) (predicted impact of computers on society over next twenty years). In 1976, computers provided jobs for more than two million people in the United States as programmers, operators, and maintenance technicians. Volgyes, *The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review*, 2 COMP. L.J. 385, 386 (1980) [hereinafter cited as Volgyes]. The total number of computers in the United States should double by 1985. *Id.*

[3] *See* United States v. Jones, 553 F.2d 351, 353 n.6 (4th Cir.) (dictum that computer crime is increasing rapidly), *cert. denied*, 431 U.S. 968 (1977). *See generally* D. PARKER, CRIME BY COMPUTER 23-40 (1976) [hereinafter cited as PARKER]; Swanson & Territo, *supra* note 2.

[4] Prosecutors at the state level usually have attempted to prosecute computer crimes under two general areas of criminal law. *See* A. BEQUAI, COMPUTER CRIME 25 (1978) [hereinafter cited as BEQUAI]. First, state prosecutors have been able to secure convictions by alleging various offenses involving habitation. *Id.* Included in the habitation category are arson and burglary. Habitation offenses usually occur when the computer is the object of a crime. *Id.* at 25-28; *see* text accompanying notes 12-13 *infra*. Additionally, prosecutors have found that statutes prohibiting certain offenses against property are applicable to many computer crimes. *Id.* at 28. The property category includes larceny, embezzlement, false pretenses, extortion, malicious mischief, forgery, and receipt of stolen property. *Id.* at 28-34. The successful prosecution of computer crimes as offenses against property in a particular state initially will depend on whether the data, program, or equipment falls within the state's definition of property. *See* Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMP. L.J. 353, 376 (1980) [hereinafter cited as Sokolik]; *see, e.g.*, ARIZ. REV. STAT. ANN. § 13-2301 E. 8 (Supp. 1980); CAL. PENAL CODE § 502(7) (Supp. 1980) (West); VA. CODE § 18.2-98.1 (Supp. 1980).

Attempts to prosecute computer crimes at the federal level usually have employed the federal mail fraud statute in 18 U.S.C. § 1341 (1976). *See* United States v. Curtis, 537 F.2d 1091, 1093 (10th Cir.), *cert. denied*, 429 U.S. 962 (1976); United States v. Kelly, Crim. #77-250 (E.D. Pa. 1977); BEQUAI, *supra*, at 37-38. For the mail fraud statute to apply, the criminal must have used the United States Postal Service in a fraudulent scheme. 18 U.S.C.

ment techniques often has restricted law enforcement in the computer field.[5] A number of United States legislators have proposed federal legislation[6] as a means of managing the fertile areas for crime created by the continued inundation of society by computer technology.[7] Although

---

§ 1341 (1976). Another drawback to the application of the mail fraud statute to computer crime is that the maximum penalty available under § 1341 is a $1000 fine and five years in prison, even though the crime may have involved significantly larger sums of money. *Id.*; *cf.* text accompanying note 57 *infra.*

Other federal statutes that have been useful in the prosecution of computer crime are the statutes prohibiting fraud perpetrated through interstate communication wires, 18 U.S.C. § 1343 (1976), statutes prohibiting the receipt and interstate transportation of stolen securities, 18 U.S.C. §§ 2314-15 (1976), the bank crime statutes, 18 U.S.C. §§ 656-57 (1976), and the federal embezzlement and theft statute, 18 U.S.C. § 641 (1976). *See* United States v. Seidlitz, 589 F.2d 152, 153 (1978) (conviction under wire fraud statute), *cert. denied*, 441 U.S. 922 (1979); United States v. Jones, 553 F.2d 351 (4th Cir. 1977) (applicability of securities laws to computerized check thefts); United States v. Lambert, 446 F. Supp. 890, (D. Conn. 1978) (applicability of federal embezzlement statute to information derived from government computer); United States v. Sampson, 6 COMP. L. SERV. REP. 879, 880 (N.D. Cal. 1978) (federal embezzlement statute applied to theft of computer time). *See generally* Volgyes, *supra* note 2, at 394-399.

[5] *See* text accompanying notes 23-51 *infra.*

[6] *See* Federal Computer Systems Protection Act (FCSPA), S. 240, 96th Cong., 2d Sess. (1980); H. R. 6192, 96th Cong., 1st Sess., 125 CONG. REC. H. 12352 (daily ed. Dec. 19, 1979) [hereinafter cited as FCSPA].

[7] The foremost reason for the computer's exceptional vulnerability to crime is that each stage in a computer's operation provides opportunities for the enterprising criminal. *See* BEQUAI, *supra* note 4, at 9; Gammer, *Computer Crime*, 18 AM. CRIM. L. REV. 370, 372-74 (1980) [hereinafter cited as Gammer]. By altering the input on which the computer will operate, the criminal can control the form and content of the computer product. *See* BEQUAI, *supra* note 4, at 9-10. By inputting false data into the computer, the criminal can cloak his crime in the seemingly legitimate form of computer output. *See* PARKER, *supra* note 3, at 21 (computer used as a symbol to intimidate, deceive, or defraud). Moreover, since input mistakes are common, the criminal can blame any discovered alterations of input on unintentional error. *See* BEQUAI, *supra* note 4, at 10.

Programming is the next stage of computer operation. *See id.* The program is the instructions the computer follows to perform the particular desired task. *See id.* By manipulating the computer program, the criminal can control the actual operation of the computer without having to alter the input to achieve a fraudulent result. *See id.* To the extent that the overall program is likely to be very complex, program changes are extremely difficult to locate. *See id.*

Of less importance to the ordinary criminal is the central processing unit (CPU) stage of the computer's operation. The CPU provides the core intelligence for the basic computer functions of information storage and retrieval, and reading, decoding, and following the chosen program. *See id.* The CPU is not readily alterable as are computer input and programs. Since the CPU is not easily manipulated for criminal purposes, the CPU's potential role in a crime is as a possible target for terrorists or the object of vandalism or theft. *See id* at 10-11; Roddy, *The Federal Computer Systems Protection Act*, 7 RUTGERS J. OF COMP., TECH. AND THE L. 343, 348 (1980) [hereinafter cited as Roddy] (any type of induced CPU malfunction could effectively ruin computer user by destroying data bases).

The next stage of computer operation is output. Output is normally valuable to the computer criminal for the information the output contains. *See id.* Thus, the output is most likely to be the object of theft, rather than manipulation. *See* BEQUAI, *supra* note 4, at 11.

The final stage in computer operation is the communication process. *See id.* The com-

the proposed legislation creates clearly applicable legal sanctions for most computer improprieties,[8] the legislation does not provide for increased prevention, detection, and reporting of computer crime.[9] A legislative attempt to control computer crime should go beyond merely identifying and prohibiting certain activities.

The term "computer crime" encompasses a broad range of activities.[10] In general, computer crime consists of volitional, nonviolent acts involving a computer. The acts cause someone to suffer or potentially suffer damage, and through these criminal acts the perpetrator receives or could receive a benefit.[11] There are four general categories of computer crime.[12] The first type of computer crime occurs when the computer is the object of some illicit activity.[13] Sabotage or theft of the computer are examples of crimes involving the computer as the object of the crime.[14] Situations in which the computer provides the necessary environment for the crime comprise the second type of computer crime.[15] For example, although theft or destruction of computer programs may be a serious loss to a company,[16] the value of a computer program without a computer is negligible.[17] The third variety of computer crime occurs when the computer is the instrument of the crime.[18] Anytime a criminal uses the computer's data processing capabilities to perpetrate a crime, the computer is an instrument of the crime.[19] An example of this type of crime is programming a computer to write checks automatically to an unauthorized payee.[20] The final category of computer crime involves us-

---

munication process refers to the transmission of data, whether input or output, to and from remote terminals and computers. *See id.* The principal opportunities for crime in the communications process involve interception of data and unauthorized use of a computer through access to a remote terminal. *See id.*; Roddy, *supra*, at 348-49.

[8] *See* FCSPA, *supra* note 6; *supra* note 2; Sokolik, *supra* note 4, at 378.

[9] *See* text accompanying notes 66-76 *infra*.

[10] *See generally* PARKER, *supra* note 3, at 12-22.

[11] *See* McLaughlin, *Computer Crime: The Ribicoff Amendment to United States Code, Title 18*, 2 CRIM. JUST. J. 217, 219-20 (1979) [hereinafter cited as McLaughlin]; *accord 1980 Hearings, supra* note 2, at 10 (remarks of Colo. Attorney General MacFarlane) (computer crime is crime involving use or operation of computers).

[12] *See* Gemignani, *Computer Crime: The Law in '80*, 13 IND. L. REV. 681, 682-83 (1980) [hereinafter cited as Gemignani].

[13] *See* PARKER, *supra* note 3, at 17-19; Gemignani, *supra* note 12, at 682.

[14] *See* PARKER, *supra* note 3, at 211-27 (situation involving computer sabotage).

[15] *See id.* at 19-20; Gemignani, *supra* note 12, at 682-83.

[16] A business' expenditures for computer programs often represent more than half of the total investment required for electronic data processing operations. *1980 Hearings, supra* note 2, at 27 (statement of Michael Dertouzos).

[17] *Cf.* Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967) (court refused to accept valuation of computer program based on the value of paper on which program was printed).

[18] *See* PARKER, *supra* note 3, at 20-21; Gemignani, *supra* note 12, at 683.

[19] *See* PARKER, *supra* note 3, at 20.

[20] *See* United States v. Jones, 553 F.2d 351, 353 (4th Cir. 1977) (altered input causing issuance of unauthorized checks).

ing a computer as a symbol in the perpetration of a crime.[21] The use of computerized documents to add an aura of authenticity to a fraudulent scheme represents the symbolic presence of a computer in a crime.[22]

Although the many types of computer crimes pose obvious threats to society, control of computer crime is often very difficult.[23] Statistics indicate that only 1 in every 100 computer crimes are detected.[24] Moreover, the risk of prosecution for a computer crime is only 1 in 22,000.[25] Despite the low risk, the potential yield from computer crime is high.[26] One study states that the average proceeds from a computer crime are $450,000.[27] While the average bank robbery results in a $10,000 loss, computer bank frauds average $193,000 per incident.[28] The magnitude of the possible yield coupled with the relatively low risk illustrates the attractiveness of the computer to existing and potential criminals.

While the opportunity for low risk-high yield crime has grown as computer use has become more widespread,[29] the capabilities of law enforcement officials to fight computer crime have not improved with the same speed.[30] The first hurdle confronting law enforcement officials is the detection of existing crimes.[31] The low visibility of most computer crime[32] makes discovery of such crimes through police initiated action difficult.[33] Sources outside of law enforcement agencies ordinarily bring about investigations by reporting detected incidents.[34] Unfortunately, only 1 in 5 detected computer crimes are reported.[35] The reluctance of those persons who discover computer improprieties to report discoveries impedes police attempts to control computer crime.[36]

---

[21] *See* PARKER, *supra* note 3, at 21-22; Gemignani, *supra* note 12, at 683.

[22] *See* United States v. Curtis, 537 F.2d 1091, 1093 (10th Cir. 1976) (manually maintained dating service advertised as being "computerized").

[23] *See* text accompanying notes 29-51 *infra*.

[24] *Federal Computer Systems Protection Act: Hearings on S. 1766 Before the Subcomm. on Criminal Laws and Procedures of the Judiciary*, 95th Cong., 2nd. Sess. 4 [hereinafter cited as *1978 Hearings*] (statement of Senator Biden).

[25] Swanson & Territo, *supra* note 2, at 305; Volgyes, *supra* note 2, at 388.

[26] *See* Volgyes, *supra* note 2, at 386-87.

[27] *See* Gemignani, *supra* note 12, at 686; Taber, *A Survey of Computer Crime Studies*, 2 COMP. L.J. 275, 307 (1980) [hereinafter cited as *Survey*].

[28] *1978 Hearings*, *supra* note 24, at 18 (statement of Senator Percy).

[29] *See* Volgyes, *supra* note 2, at 386.

[30] *See 1978 Hearings*, *supra* note 22, at 24 (discussion between Senators Biden and Percy).

[31] *See* Volgyes, *supra* note 2, at 395.

[32] *See* Sokolik, *supra* note 4, at 359; note 85 *infra*.

[33] *See 1980 Hearings*, *supra* note 2, at 10 (remarks of Colo. Attorney General MacFarlane).

[34] *1978 Hearings*, *supra* note 24, at 33 (remarks of F.B.I. Chief Hennehan) and 46 (remarks of Senator Biden). Examples of sources outside of law enforcement agencies that report computer improprieties are auditors, informants, and suspicious business managers.

[35] *Id.* at 18 (statement of Senator Percy); *cf.* Swanson & Territo, *supra* note 2, at 305 (15% of computer crimes are detected and reported).

[36] *1978 Hearings*, *supra* note 24, at 11 (statement of Senator Ribicoff).

Once reported, a computer crime continues to pose problems to law enforcement officials during investigation. The complex computer technology that helps to camouflage criminal activity[37] may confound the ordinary detective.[38] Computer crime often involves complex technological concepts.[39] To conduct an investigation of a computer crime, a detective may need special training to understand the particular crime.[40] Frequently, local law enforcement agencies are reluctant or unable to commit the resources necessary to provide skills in basic computer crime investigation.[41] Even at the federal level, formal courses in computer crime investigation are recent additions to police training curricula and the courses are limited to relatively few agents.[42] The overall lack of technical training puts the police at a major disadvantage in dealing with the computer criminal.[43]

In addition to problems at the detection and investigation stages, complications also arise in prosecuting a computer crime. Only a few states have statutes specifically directed at computer crime.[44] Federal prosecutors have no directly applicable code provisions upon which to rely,[45] but the United States Code contains 40 sections that federal prosecutors can adapt to computer crime.[46] As a result, most state and all federal prosecutors must charge computer criminals for other crimes that may apply in the computer situation.[47] Although the statute may

---

[37] *See* Sokolik, *supra* note 4, at 359. Since the computer usually stores data in machine-readable forms only and data processing takes place within the computer, the investigator ordinarily lacks the opportunity to examine questionable documents without alerting the operators of the computer system. *See* Roddy, *supra* note 7, at 349.

[38] *See* State v. Thommen, No. 79-424B (Crim. Ct. Marion Co., Ind. Feb. 14, 1980), *reviewed by* Gemignani, *supra* note 12, at 713-18. In *Thommen*, the defendant was convicted of the thefts of computer time. Gemignani, *supra* note 11, at 713-15. The nature of Thommen's crime was so complex, however, that an investigator trained in computer crime investigation spent nearly a year trying to understand the unauthorized activities after the improprieties surfaced. *Id.* at 715.

[39] *See* Gammer, *supra* note 7, at 373 n.1744.

[40] *See 1978 Hearings*, *supra* note 24, at 43-44 (discussion between Senator Biden and F.B.I. Chief Barko).

[41] *See* BEQUAI, *supra* note 4, at 57. *Compare 1980 Hearings*, *supra* note 2, at 10 (remarks of Colo. Attorney General MacFarlane) (technical expertise at local law enforcement level not needed) *with 1980 Hearings*, *supra* note 2, at 54 (statement of National District Attorneys Ass'n Chairman Falke) (necessity of specialized expertise).

[42] *See 1978 Hearings*, *supra* note 24, at 34 (statement of F.B.I. Chief Hennehan).

[43] *See id.* Although law enforcement officials generally lack technical training in the computer field, computer criminals are usually well educated and technically competent. *See* BEQUAI, *supra* note 4, at 4.

[44] *See generally* Krieger, *Current and Proposed Computer Crime Legislation*, 2 COMP. L.J. 721 (1980).

[45] *1978 Hearings*, *supra* note 24, at 11 (statement of Senator Ribicoff).

[46] *See* note 4 *supra*.

[47] *See, e.g.*, United States v. Seidlitz, 589 F.2d 152, 155 (4th Cir. 1978); United States v. Jones, 553 F.2d 351, 355 (4th Cir. 1977). In *Seidlitz*, the defendant was accused of the unauthorized use of a former employer's computer. 589 F.2d at 155. The defendant had gain-

prohibit the particular conduct involving the computer, the elements of the crime and the sanctions imposed for commission of the crime are not tailored to the computer setting.[48] Not only do prosecutors often encounter difficulty fitting the facts of a computer incident into the elements of a more traditional crime,[49] but often the punishment provided for the crime is not commensurate with the gravity of the crime in a computer context.[50] The lack of prohibitions specifically applicable to computer crime often hinders attempts to bring the computer criminal to justice.[51] In short, law enforcement officials are likely to have problems at every stage of the fight against computer crime.

The criminal potential of the computer and the problems associated with the detection and prosecution of computer crimes led to the introduction in 1977 of the Federal Computer Systems Protection Act (FCSPA).[52] As revised in 1980,[53] the FCSPA would prohibit the use or attempted use of a computer,[54] either as an instrument or a sym-

---

ed access to the computer, which was located in Maryland, by telephone through terminals located in Virginia and Maryland. *Id.* at 154-55. Although the trial court convicted the defendant of perpetrating a fraud through interstate wires, 18 U.S.C. § 1343 (1976), the trial court dismissed as inapplicable the count of the indictment charging the defendant with interstate transportation of stolen property. 589 F.2d at 155 n.12; *1978 Hearings, supra* note 24, at 29 (statement of Deputy Assistant Attorney General Keeney). If the defendant had accessed the computer only from the location in Maryland, conviction under federal law would have been unlikely. *See* Roddy, *supra* note 7, at 355.

In *Jones*, the defendant's accomplice altered input data to instruct the computer to write unauthorized checks to the order of the defendant. 553 F.2d at 353-54. The defendant was charged with the interstate transportation of fraudulently obtained checks in violation of 18 U.S.C. §§ 2314-15 (1976). 553 F.2d at 352. The trial court dismissed the charges on the ground that the checks were forgeries which are expressly excluded from the provisions of the federal statute. United States v. Jones, 414 F. Supp. 964, 971 (D. Md. 1976); *see* 18 U.S.C. §§ 2314-15 (1976). The circuit court reversed the dismissal stating that the issuance of the check by the computer made the check a fraud rather than a forgery. 553 F.2d at 356. Thus, the checks did not come within the exceptions to 18 U.S.C. §§ 2314-15 (1976). 553 F.2d at 356.

[48] *See* Sokolik, *supra* note 4, at 371-73.

[49] *See* United States v. Jones, 553 F.2d 351, 355-56 (appellate court reversal of trial court finding that computer written check to unauthorized payee constituted forgery).

[50] *See* BEQUAI, *supra* note 4, at 5-6.

[51] *See 1978 Hearings, supra* note 24, at 28 (statement of Deputy Assistant Attorney General Keeney).

[52] S. 1766, 95th Cong., 1st Sess., 123 CONG. REC. 21025 (1977).

[53] S. 240, 96th Cong., 2nd Sess. (1980). *See generally* McLaughlin, *supra* note 11; Roddy, *supra* note 7; Comment, *Computer Crime—Senate Bill S. 240*, 10 MEM. ST. U.L. REV. 660 (1980). S. 240 received the unanimous approval of the Senate Subcommittee on Criminal Law on November 6, 1979. The bill has not received the approval of the Senate Judiciary Committee. *See* Gammer, *supra* note 6, at 382 n. 1826, 384. Although Congress has yet to enact the FCSPA, the bill has served as a model for most recent state legislation in the computer crime area. *See* Becker, *The Trial of a Computer Crime*, 2 COMP. L.J. 441, 447 (1980); *see, e.g.*, ARIZ. REV. STAT. ANN. §§ 13-2301, 13-2316 (1978); MICH. COMP. LAWS ANN. § 752.791-.797 (Supp. 1980); R. I. GEN. LAWS § 11-52-1 to 4 (Supp. 1979).

[54] The FCSPA defines "computer" as any device that performs "logical, arithmetic, and storage functions by electronic manipulation." S. 240, 96th Cong., 2nd Sess. § 3(c)(1)

bol,[55] for any fraudulent purpose.[56] The FCSPA provides a maximum penalty for violation of these prohibitions of 5 years imprisonment and a fine equal to twice the amount of gain derived from the crime or $50,000, whichever is greater.[57] The FCSPA also prohibits the unauthorized, intentional damaging of a computer.[58] The maximum penalty for causing prohibited computer damage is 5 years in prison and a fine of $50,000.[59] The prohibitions of the FCSPA apply to any computer used by the federal government[60] or any financial institution[61] and all computers which affect interstate commerce.[62] The enumerated categories cover virtually every computer operated in the United States.[63] To avoid discouraging state and local attempts to control computer crime, the FCSPA provides for concurrent federal, state, and local jurisdiction over individual computer crimes.[64] The overall thrust of the FCSPA is to deter computer crime through imposition of direct legal sanctions for most computer crimes.[65]

As a major means of controlling computer crime, the present provisions of the FCSPA are inadequate. If computer crime is serious enough to warrant legislative attention,[66] the drafters of the FCSPA have only

---

(1980). The definition of computer includes peripheral equipment that is connected to or operates with a computer. *Id.* For purposes of the FCSPA, automated typewriters, household-type micro-computers, and hand-held calculator's are excluded expressly from the definition of a computer. *Id.*

[55] *See* text accompanying notes 19 & 21 *supra.*

[56] S. 240, 96th Cong., 2nd Sess. § 3(a) (1980).

[57] *Id.* at § 3(a)(2).

[58] *Id.* at § 3(b).

[59] *Id.*

[60] *Id.* at § 3(a)(1)(A).

[61] *Id.* at § 3(a)(1)(B).

[62] *Id.* at § 3(a)(2). The authors of the FCSPA intended the term "operates in interstate commerce" to have an expansive meaning. *1978 Hearings, supra* note 24, at 25 (remarks of Senator Biden).

[63] *See 1980 Hearings, supra* note 2, at 4 (statement of Senator Laxalt); Roddy, *supra* note 7, at 350.

[64] S. 240, 96th Cong., 2nd Sess. § 3(d). The FCSPA provides that federal prosecutors should use discretion in deciding whether to exercise jurisdiction over a computer crime that also falls within state or local jurisdiction. *Id.* The bill states that a federal official's decision whether to exercise jurisdiction should include consideration of the gravity of the offense, the extent of federal interest in the crime, the resources available to state and local authorities, and the traditional federal role with respect to the crime. *Id.* The provisions calling for federal discretion in exercising jurisdiction were not part of the earlier versions of the FCSPA. *See* S. 1766, 95th Cong., 1st Sess. (1977). The addition of the provisions probably resulted from suggestions by critics of the bill that the broad grant of federal jurisdiction in the FCSPA unnecessarily injects the federal government into situations that are essentially local. *See 1980 hearings, supra* note 2, at 53-54 (statement of National District Attorneys Ass'n Chairman Falke).

[65] *1978 Hearings, supra* note 24, at 6 (statement of Senator Ribicoff).

[66] At least one commentator argues that a computer crime is actually nothing more than a standard crime with the computer as one component of the factual setting. Taber, *On Computer Crime (Senate Bill S. 240)*, 1 COMP. L.J. 517, 537 (1979) [hereinafter cited as

partially addressed the problem.[67] Although prosecutors of computer crimes have had to rely on tangentially related criminal statutes,[68] virtually no criminal prosecution has failed for lack of statutory sanction.[69] A district attorney, however, cannot prosecute an undiscovered or unreported computer crime. Furthermore, any preventive or deterrent effect of clearly applicable, strict penalties exists only to the extent that the courts are able to apply the penalties to detected illegal acts.[70] Thus, the solution to the problem of rising computer crime should couple measures directed toward detection and prevention with the creation of direct legal sanctions.[71]

In addition to prevention and detection, a legislative attempt to control computer crime should address the public's reluctance to report discovered computer crimes. The usual response to increased crime is increased government spending on law enforcement in the affected area.[72] Undoubtedly, increased funding of law enforcement projects on computer crime would facilitate the investigation and prosecution of reported incidents.[73] As in many areas of whitecollar crime,[74] however, investigations of computer crime are limited to cases in which unofficial

---

Taber]. The same authority also argues that the results of studies measuring computer crimes are statistically invalid. *Id.* at 523. *See generally* Survey, *supra* note 27. Above all, the authority contends that assuming the validity of computer crime statistics, computer crime is insignificant in comparison to white-collar crime as a whole. Taber, *supra*, at 518. *See generally* PARKER, *supra* note 3, at 294-95.

[67] *See* Sokolik, *supra* note 4, at 373-74 (sponsors of FCSPA have limited objectives in legislation).

[68] *See* note 4 *supra*.

[69] *1980 Hearings*, *supra* note 2, at 4 (statement of Senator Laxalt); *see id.*, *supra* note 2, at 10 (statement of Colo. Attorney General MacFarlane) (detection, not prosecution, poses largest problem in controlling computer crime).

[70] *1978 Hearings*, *supra* note 24, at 112 (letter of Deputy Assistant Attorney General Keeney).

[71] One example of legislation that coupled provisions criminalizing certain acts with provisions specifically aimed at prevention and detection of the prohibited act is the Antihijacking Act of 1974, PUB. L. NO. 93-366, 88 Stat. 409 (codified in scattered sections of 49 U.S.C.). Under the Antihijacking Act, Congress provided stiff penalties for anyone who hijacks or attempts to hijack an airplane. 49 U.S.C. § 1472(n) (1976). The Air Transportation Security Act of 1974, PUB. L. NO. 93-366, 88 Stat. 415 (codified in scattered sections of 49 U.S.C.) provided for the promulgation of regulations for the screening of passengers for weapons and the implementation of strict airport security measures. *Id.* §§ 1356-57. Congress authorized the Federal Aviation Administration to conduct research and development projects designed to protect passengers and property from air piracy. *Id.* § 1357(d)(1).

[72] *See* S. REP. NO. 1097, 90th Cong., 2nd Sess. 1-9, *reprinted in* [1968] U.S. CODE CONG. & AD. NEWS 2112, 2115-23. In 1968, Congress responded to reports of growing crime in the United States by establishing the Law Enforcement Assistance Administration to administer grants to individual states to fight crime. *Id.* at 2114-16.

[73] *See 1978 Hearings*, *supra* note 22, at 34 (statement of F.B.I. Chief Henehan) (F.B.I. does not have adequate investigative resources to deal with all types of computer crime).

[74] Computer crime is one variety of white-collar crime. Volgyes, *supra* note 2, at 387. White-collar crime is usually characterized as nonviolent illegal acts perpetrated by deceit or concealment. A. BEQUAI, WHITE-COLLAR CRIME: A 20TH-CENTURY CRISIS 1-3 (1978).

sources report alleged improprities to the authorities.[75] The scarcity of detected and subsequently reported crimes would limit the impact of successful investigations that increased funding would make possible.[76] Thus, since effective enforcement of computer crime laws depends, in large part, on increased reporting of discovered crimes, Congress should encourage those who uncover computer improprieties to report to law enforcement authorities.

Assuming that legislation should include measures directly aimed at prevention, detection, and reporting of computer crime, attention must focus on what available alternatives would accomplish these three objectives. The prevention and detection of computer crime depends almost entirely on the adequacy of computer security measures.[77] Reporting discovered computer irregularities[78] simply depends upon the decision of the discoverer to take appropriate action when an incident occurs. Therefore, legislation directed toward improving prevention, detection, and reporting must focus on the persons involved in the design and operation of computers who have responsibility for overseeing security procedures and who are most likely to discover computer improperties. The three groups that meet these qualifications are the users of computers,[79] the manufacturers of computers,[80] and the outside auditor of

---

[75] *See* text accompanying notes 32-34 *supra.*

[76] *See* text accompanying notes 29-33 *supra.*

[77] *See* BEQUAI, *supra* note 4, at 19; PARKER, *supra* note 3, at 275-76; Sokolik, *supra* note 4, at 368-70. Computer security measures fall into four general categories. *See generally* J. CARROLL, COMPUTER SECURITY (1977) [hereinafter cited as CARROLL]; L. KRAUSS & A. MACGAHAN, COMPUTER FRAUD AND COUNTERMEASURES (1979) [hereinafter cited as KRAUSS & MACGAHAN]. The first category is comprised of physical controls. Physical controls include regulations governing actual physical access to computer, programs, data, and output. Management of the computer's physical environment is also a physical control. *See* CARROLL, *supra*, at 81-94; KRAUSS & MACGAHAN, *supra* at 115-21. Communications controls are another category of security measures. Any method designed to protect data transmission, such as a device that prevents or detects wiretapping, is a communications control. *See* CARROLL, *supra* at 139-205. The next variety of security methods is systems controls. Systems controls may involve isolation of individual components of the computer system through the use of user logs and time allotments. Restricted circulation of operations manuals or programs that control user access are also systems controls. *See* KRAUSS & MACGAHAN, *supra*, at 179-190. The final category is hardward controls. Hardward controls are mechanical controls builts into the computer to lessen the opportunity for improper use of the computer. *See* PARKER, *supra* note 3, at 276. Examples of hardward controls are machine-maintained logs of individual user numbers and times and restrictions on acceptable programming languages. *See* KRAUSS & MACGAHAN, *supra*, at 190-95.

[78] The term "irregularities" is an auditing term connoting all intentional misrepresentations, misappropriations, and defalcations. American Institute of Certified Public Accountants (AICPA) Professional Standards AU § 327.03.

[79] In general, the term "users" refers to users of computers in the private sector. Government computer operations are subject to regulations and security procedures that do not apply to computer systems in the private sector. *See, e.g.*, 5 U.S.C. § 552 (1976) (regulation of the collection, storage and dissemination of personal information by federal agencies); 41 C.F.R. §§ 101-36.000 to 36.1207 (1980) (regulations governing management of automatic data processing equipment used by the federal government).

[80] *See* text accompanying notes 97-110 *infra.*

computer users.[81] Each group possesses a different potential for having an impact on each of the three objectives of prevention, detection, and reporting.

The users of computer systems have the largest stake in preventing and detecting computer crime.[82] The costs and uncertainties associated with computer crime have an immediate effect on the user.[83] Moreover, the user is in the best position to develop and implement basic security measures for the computer system.[84] Although implementation and maintenance of proper external security measures would prevent most computer crimes,[85] users of computers generally have failed to initiate

---

[81] The auditor's certification that a business' financial statements represent fairly the financial condition of the company plays a major role in the business community. *See* Besser, *Privity?—An Obsolete Approach to the Liability of Accountants to Third Parties*, 7 SETON HALL L. REV. 507, 507 (1976) [hereinafter cited as Besser]. *See generally* Comment, *Accountant's Liability for Negligence—A Contemporary Approach For a Modern Profession*, 48 FORDHAM L. REV. 401, 401-08 (1979) [hereinafter cited as *Contemporary Approach*]. Not only do many creditors and investors in small business rely on the auditor's opinion, the opinion is a necessity to virtually all medium and large companies. Federal securities laws require all companies with more than 500 shareholders and more than $1,000,000 in total assets to file audited financial statements with the Securities Exchange Commission (SEC). 15 U.S.C. §§ 78l(g)(1)(B) & 78m(a)(2) (1976).

[82] In 1974, the United States Chamber of Commerce estimated that annual losses attributable to computer crime exceeded $100 million. *1978 Hearings, supra* note 24, at 57 (statement of Donn Parker). Current estimates of annual losses due to computer crime range as high as $300 million. *See* Swanson & Territo, *supra* note 2, at 305.

[83] Direct financial losses are only part of the detrimental effect that computer crime has on the user. Computer crime also results in a distortion of financial statements which causes economic dislocation as managers try to cure fictitious financial problems. *See* KRAUSS & MACGAHAN, *supra* note 77, at 23-24 (fraudulent debits). Also, in many cases the victim may not even miss the property that is the subject of the computer crime. Nevertheless, the crime may result in the deterioration of the user's competitive position. For instance, criminal access to a trade secret stored in a computer could do irreparable harm to the owner of the secret. *See* Ward v. Superior Court, 3 COMP. L. SERV. REP. 206 (Super. Ct. Cal. 1972) (theft by telephone of computer program from one computer service company by employee of another computer service company).

[84] *See* note 77 *supra*. Although the computer user may not be capable of installing hardware controls, only the user can require that purchased computer systems have adequate hardware controls. *See* text accompanying notes 102-04 *infra*.

[85] *See* text accompanying note 77 *supra*. In addition to the obvious direct effect of security measures, the implementation and enforcement of standard security procedures also provides an indirect impetus to computer crime detection. Although even the best crime prevention techniques cannot ensure crime-free operation of all computer systems, a comprehensive prevention plan deprives the computer criminal of the natural camouflage of the computer. *See* Sokolik, *supra* note 4, at 370 (prevention techniques provide greater capacity for early discovery of wrongdoings). Much of the present problem of computer crime stems from the ability of the criminal to use the computer as an anonymous tool in the perpetration of crime. *See* Volgyes, *supra* note 2, at 393; note 37 *supra*. By creating internal and external documentation of all computer operations and controlling access to the computer system, security procedures not only deter the criminal, but also provide a trail for audit or investigation if suspicions about an employee's activities arise. *See* KRAUSS & MACGAHAN, *supra* note 77, at 345 (sources of investigation).

proper security measures in the operation of their computer systems.[86] Even when users implement proper security measures, a lack of maintenance and enforcement of existing security procedures can undermine the security system's effectiveness in crime detection.[87] Furthermore, many users are reluctant to report crimes that security procedures un-

[86] *1978 Hearings*, *supra* note 24, at 33 (remarks of Joseph Henehan) & 59 (statement of Donn Parker); *see* PARKER, *supra* note 3, at 284; McLaughlin, *supra* note 11, at 232-33; Sokolik, *supra* note 4, at 368. The failure of computer users to provide adequate controls stems, in part, from the complexity of the computer. *See* Roddy, *supra* note 7, at 346; Sokolik, *supra* note 4, at 392. While computer technology has accelerated over the past thirty years, top management has left the details of operation of the computer to the systems analysts and programmers who understand the system. *See* Roddy, *supra* note 7, at 346; Swanson & Territo, *supra* note 2, at 305. Unfortunately, by placing responsibility for security in the hands of employees versed in computer technology, management places trust in employees who are unlikely to have training in auditing and security techniques, but are best able to perpetrate fraud. *See* Sokolik, *supra* note 4, at 366. In such a scheme, the dishonest employee has a vested interest in not recommending effective security controls whereas the honest employee sees no need for controls.

The more top management disassociates itself with the day-to-day operation of the company's computer system, the more reliance on the quantitative indications of computer performance grows. *See generally* R. THIERAUF, DATA PROCESSING FOR BUSINESS AND MANAGEMENT 573-604 (1973) (computer security expenditures as function of desired degree of accuracy and acceptable cost). Management ordinarily views the installation of a computer as a means of processing data more efficiently than a manual system. Thus, the costs associated with the operation and maintenance of the computer are an all-important measure of the system's performance. *See* Sokolik, *supra* note 4, at 370-71. The ordinarily invisible nature of computer fraud and the immediately apparent cost of increased computer security have caused management to look askance at efforts to increase computer security. *See* KRAUSS & MACGAHAN, *supra* note 77, at 411-12; Sokolik, *supra* note 4, at 370. The general lack of appreciation for the devastating opportunities the computer offers to the technologically inclined criminal reinforces management's reluctance to increase security outlays. *See* text accompanying notes 24-28 *supra*; *1978 Hearings*, *supra* note 24, at 65 (remarks of Donn Parker).

Although inaction on the part of computer users has contributed to a lack of computer crime prevention in the past, there are indications of a growing awareness of the problem and resultant attempts to deal with it. *Id.* Increased public awareness of the criminal propensities of the computer has resulted from recent revelations of massive computer frauds in major companies and government. *See, e.g.*, Hel & Lancaster, *Fraud at Wells Fargo Depended on Avoiding Computer's Red Flags*, Wall St. J., Feb. 26, 1981, at 1, col. 6; Hollie, *Police Recount Theft by Wire of $10 Million*, N.Y. Times, Nov. 8, 1978 § A, at 11, col. 1; *U.S. Aide Held in $500,000 Theft by Computer*, Wash. Post, Feb. 20, 1980 § C, at 3, col. 1. Accordingly, the activities of internal auditors with respect to computer systems and the interest of the audit committees of boards of directors have increased dramatically. *See 1978 Hearings*, *supra* note 24, at 82-83 (remarks of Robert Abbott); PARKER, *supra* note 3, at 286-87.

The federal government has recently introduced standards of security control for computers that are applicable to all branches of the federal government. *See* note 79 *supra*. To the extent that increased awareness by computer users results in concrete improvements in security controls, computer crime prevention will benefit. *See* Volgyes, *supra* note 2, at 402. Thus far, however, computer crime statistics indicate that voluntary measures to control computer crime have been unsuccessful. *See* text accompanying notes 23-28 *supra*.

[87] *See* BEQUAI, *supra* note 4, at 22-23.

cover.[88]

Reluctance on the part of computer users to adopt voluntary security measures to prevent computer crime does not suggest that involuntary requirements are a workable alternative. The original hearings on the FCSPA[89] indicated that licensing of individual computer systems is an unacceptable method of ensuring compliance with minimum security procedures.[90] Standard procedures that are applicable to the myriad of possible computer users would be virtually impossible to develop.[91] Once developed, government attempts to require the user to maintain and enforce the security procedures would result in a regulatory quagmire. In short, government attempts to stimulate crime prevention and detection in users of computers may be limited to efforts to increase public awareness of the computer's potential for crime.[92]

Although mandatory security requirements are impractical, mandatory reporting requirements for users would be relatively simple to develop.[93] Nevertheless, the authors of the FCSPA considered and declined to include a provision mandating that any computer user having knowledge of a computer crime make a report to law enforcement of-

---

[88] *See* text accompanying note 35 *supra*. Among users of computers, reasons given for declining to report computer crimes include embarrassment, fear of bad publicity and resulting lack of public confidence, and potential liability to shareholders for negligent management of computer operations. *See 1978 Hearings*, *supra* note 24, at 11 (statement of Senator Ribicoff) & 28 (statement of Deputy Assistant Attorney General Keeney); Volgyes, *supra* note 2, at 388. Another, less likely reason for the failure to report cases is the opportunity for personal gain from joining forces with the computer criminal. *See* Swanson & Territo, *supra* note 2, at 306.

[89] *See* note 24 *supra*.

[90] *See 1978 Hearings*, *supra* note 24, at 51-52 (statement of Senator Biden). At the 1978 Hearings, Senator Biden dismissed the alternative of licensing computer users without giving reasons for his remarks. *Id.* The Senator's reticence on the subject of licensing probably stemmed from a national feeling against increased federal regulation especially in a field as pervasive as computer use. *See generally* Kennedy, *The Delegalization of America*, 28 DRAKE L. REV. 539 (1979).

[91] *See* Sokolik, *supra* note 4, at 369 (effective security system design must take into account type of required access and principal system application). The fundamental problems with mandatory security measures are the effective adaptation of standard security measures to individual situations and the enforcement of the requirements by the government. The degree of regulation necessary to solve the fundamental problems makes licensing particularly distasteful to legislators. *See 1978 Hearings*, *supra* note 24, at 51-52 (remarks of Senator Biden); note 90 *supra*.

[92] *See 1978 Hearings*, *supra* note 24, at 154 (letter of Rein Turn) (recommending special effort to giving FCSPA maximum publicity). Illustrative of legislative efforts to increase public awareness of possibly prohibited conduct are certain requirements of federal copyright law. In order to avoid possible liability for copyright infringement, libraries and archives must display a notice on all photocopy equipment warning users that making a copy may be subject to the copyright law. 17 U.S.C. § 108(f)(1) (1976).

[93] *E.g.* 21 C.F.R. § 1304.41(b) (1980) (report from distributor of controlled substances must list thefts).

ficials.[94] Reasons mentioned for non-inclusion of a reporting requirement ranged from fear of creating distrust within the affected business entity to doubts about the effectiveness of a reporting requirement.[95] These reasons do not explain adequately the total absence of provisions in the FCSPA directed toward encouraging computer users to report crimes.[96]

Unlike users of computers, the manufacturers of computer systems are in a position to play a significant role only in preventing computer crime.[97] Ideally, computers should be able to police themselves.[98] Some authorities on computer security predict that a totally secure computer system will become a reality,[99] but that security technology is currently lagging five to eight years behind data processing technology.[100] The major reason for the computer industry's failure to emphasize security innovations is the lack of enthusiasm of computer users for automated security systems.[101] Since the relationship between the manufacturer and the user of a new computer system is purely contractual,[102] the manufacturer is willing to provide only those features for which the user is willing to pay.[103] Absent express contractual provisions to the contrary, no legal theory attaches liability to the manufacturer for failure to provide built-in security features.[104] Without economic incentives or

---

[94] *See 1978 Hearings*, *supra* note 24, at 46-47 (discussion between Senator Biden and Deputy Assistant Attorney General Keeney).

[95] *See id.* at 109 (letter of Deputy Assistant Attorney General Keeney).

[96] *Cf.* McLaughlin, *supra* note 11, at 234 (legislative action designed to require reporting of computer crimes considered unlikely). At first blush, the federal misprision statute appears to criminalize any knowledge of a computer crime. The statute requires that anyone having knowledge of the commission of a felony must report the felony or be liable for up to $500 in fines and 3 years in prison. 18 U.S.C. § 4 (1976). By making the commission of computer crime a felony, the FCSPA would seem to criminalize failure to report detected crimes. The courts, however, have interpreted the misprision statute as requiring an affirmative act of concealment before criminal sanctions apply. *See, e.g.*, Branzburg v. Hayes, 408 U.S. 665, 696 n.36 (1972); United States v. Daddano, 432 F.2d 1119, 1124 (7th Cir. 1970).

[97] *See* PARKER, *supra* note 3, at 282-85.

[98] *See id.* at 284-85.

[99] *See 1980 Hearings*, *supra* note 2, at 21-22 (remarks of Michael Dertouzos); PARKER *supra* note 3, at 284. The independently secure computer would be free from human maintenance in its day to day operation. *Id.* The computer would also control any human access and monitor the physical environment surrounding the computer. *Id.* at 285.

[100] *See* PARKER, *supra* note 3, at 284; Sokolik, *supra* note 4, at 361 (eight to ten year lag).

[101] *See 1980 Hearings*, *supra* note 2, at 22 (remarks of Michael Dertouzos); PARKER, *supra* note 3, at 284.

[102] *See generally* Smith, *A Survey of Current Legal Issues Arising From Contracts For Computer Goods and Services*, 1 COMP. L.J. 475 (1979).

[103] PARKER, *supra* note 3, at 288.

[104] Courts have not extended the warranties of merchantability, Uniform Commercial Code (U.C.C.) § 2-314, and fitness for a particular purpose, U.C.C. § 2-315, to computers that fall prey to crime. Examination of analogous cases, however, indicates that the U.C.C. warranty provisions may require, under limited circumstances, manufacturer indemnification of user losses due to computer crime. In Towel Mach. Serv. Corp. v. American Uniform Ren-

legal liability, manufacturers are unlikely to strive to close the gap between data processing technology and security technology.[105]

A legislative response to the computer industry's failure to concentrate on reducing the technological gap could take two forms. First, the federal government could provide economic encouragement to the development of automated security features.[106] Just as governmental economic incentives provided much of the impetus to the fledgling computer industry in the 1940's,[107] government grants or tax incentives would hasten automated security advancements. Second, Congress could create a statutory requirement that manufacturers provide minimum security features in all computer systems. The lack of a continuing relationship between computer manufacturers and users and the plethora of applications for any computer design, however, would limit the effectiveness of government regulation of computer design.[108] In the ab-

---

tal, Inc., 7 U.C.C. REP. 162 (Civ. Ct. N.Y. 1970), the court held the supplier of uniform lockers liable for the value of uniforms taken from the lockers. *Id.* at 163. The court found that, because a locker is inherently a security device, the supplier had breached an implied warranty of fitness for a particular purpose by supplying lockers that contained duplicate locks. *Id. But see* Platt v. American Locker Co., 7 U.C.C. REP. 476 (Civ. Ct. N.Y. 1970) (lessor of coin-operated locker not liable for theft from locker).

In Chatlos Systems, Inc., v. National Cash Register Corp., 479 F. Supp. 738 (D.N.J. 1979), the court held that an implied warranty of fitness for a particular purpose arose under a contract for the sale of a computer system. *Id.* at 743. In *Chatlos*, the computer manufacturer represented to the buyer that the computer system would perform much of the buyer's bookkeeping. *Id.* at 741. The *Chatlos* court reasoned that the manufacturer had become familiar with the buyer's business and knew that the buyer was relying on the manufacturer's skill and judgment. *Id.* at 743. Based on the implied warranty, the court held the manufacturer liable for fairly extensive consequential damages that resulted when the computer system failed to perform. *Id.* at 747.

*Towel Mach. Serv. Corp.* and *Chatlos* suggest that manufacturer liability for computer crime losses is possible. *Chatlos* indicates that an implied warranty of fitness for a particular purpose may extend to sellers of computer systems who know the intended use of the computer. To the extent that a major function of a computer may be the maintenance and storage of many of a business' assets, a computer has the inherent features of a security device. Thus, under the reasoning of *Towel Machine Service Corp.*, weaknesses in a computer system that the manufacturer knows will subject a user's assets to theft or destruction, could render the manufacturer liable for lost assets.

[105] *But see* Sokolik, *supra* note 4, at 374. One commentator contends that computer manufacturers will reorder their priorities in favor of computer security in the future. *Id.* The commentator argues that manufacturers desire to avoid liability as accessories to crime and for malpractice will force changes in emphasis in the design of computer systems. *Id.* One indication of increasing acceptance by manufacturers of responsibility for computer security is a recent $40 million project by International Business Machines (IBM) to develop greater security in the design of IBM computers. *Id.* at 369-70.

[106] *See* SOMA, *supra* note 1, at 2-3. The federal government provided demand for computers and funds for research in the early stages of computer development. *Id.* at 1-3. As computer technology has progressed, however, the flow of federal funds has diminished. *Id.* at 3.

[107] *See generally id.* at 15-21; note 106 *supra.*

[108] Most of the fundamental problems with federal regulation of user security procedures apply equally to regulation of manufacturers. *See* note 91 *supra.*

sence of a continuing relationship between a manufacturer and a user, government regulation of computer manufacturers would be ineffective because of the manufacturer's inability to see that the user has not tampered with the originally secure design.[109] Moreover, to the extent that making computer manufacturers statutorily responsible for the security of their products would lessen the incentive to progress in other areas of technology, regulation is undesirable. Economic incentives for the advancement of security technology, however, may prove more rewarding than equal investment in increased enforcement of computer crime laws.[110]

Considering the practical difficulty of user and manufacturer participation in computer crime prevention and detection,[111] the outside auditor's potential contribution gains importance.[112] To certify the financial statements of a business, the auditor must follow standard auditing procedures promulgated by the American Institute of Certified Public Accountants (AICPA).[113] One of the procedures currently required in every audit is a review of the client's system of internal control.[114] Also, the AICPA prohibits an auditor from conducting an audit without sufficient technical ability to identify and evaluate necessary control features in all aspects of the client's operations including computer systems.[115] Specifically, the AICPA requires the auditor to examine computer accounting control procedures,[116] test the client's compliance with previously implemented procedures,[117] and evaluate the adequacy of security procedures of particular computer systems.[118]

The auditor's examination does not, however, have a direct effect on

---

[109] *See* PARKER, *supra* note 3, at 283 (manufacturer ability to control security of computer ends after computer comes under control of user.)

[110] *See* text accompanying notes 72-76 and 97-101 *supra.*

[111] *See* text accompanying notes 89-92 and 106-07 *supra.*

[112] *See* PARKER, *supra* note 3, at 297 (computer security will depend principally on auditing function until development of more powerful technological solutions).

[113] KRAUSS & MACGAHAN, *supra* note 77, at 335; H. SELLIN, ATTORNEY'S HANDBOOK OF ACCOUNTING 1-27 to 1-28 (1974). The AICPA is the national professional society of certified public accountants. Over 160,000 certified public accountants currently are members of the AICPA. Letter of William S. Kanaga (Chairman of the Board, AICPA) to Robert Couch (March 10, 1981).

[114] AICPA Professional Standards AU § 320.01; *see* note 41 *supra.* The term "internal control" refers to all the measures adopted within a business to safeguard assets, ensure accuracy and reliability of financial records, and encourage operational efficiency and adherence to proscribed procedures. *Id.* § 320.09. A business' system of internal control includes measures adopted to safeguard the computer system. *Id.* § 321.02.

[115] *Id.* § 321.04.

[116] *Id.* § 321.24.

[117] *Id.* § 321.27.

[118] *Id.* § 321.31. As the size of the computer installation under examination increases, the corresponding auditing standard of care may increase as well. Bigelow, *The Accountant's Potential Legal Exposure When Providing Computer Services and Advice* (1975), *reprinted* in BIGELOW, 4 COMP. L. SERV. § 5-1, Art. 5, at 10 [hereinafter cited as Bigelow]; *see* text accompanying notes 122-25 *infra.*

the outcome of the audit. The auditor's examination of the client's computer security controls is not designed to detect all potential computer crimes.[119] Instead, the quality of the client's internal control helps to determine the extent of testing the auditor must perform to certify that the client's statements fairly represent the company's condition.[120] The AICPA does not require the auditor to state a conclusion on the vulnerability of the client's computer system to criminals.[121] If fraud surfaces within the business, the degree of professional care exercised in performing the audit will determine the auditor's liability for negligence.[122]

---

[119] AICPA Professional Standards AU § 327.11. *See generally id.* § 327.

[120] *Id.* § 320.01. *See* Adams v. Standard Knitting Mills, Inc., 623 F.2d 422, 431 (6th Cir. 1980) (auditor's review of client's computer security measures not designed primarily to discover weaknesses in internal control).

[121] Although the auditor need not give an opinion on the overall integrity of the client's system of internal control to certify the client's financial statements, the client can engage the auditor to conduct a formal review of the client's internal control. *See* AICPA Statement on Auditing Standards No. 30 (superceding AICPA Professional Standards AU §§ 640 & 641) [hereinafter cited as SAS 30] (reporting on internal control).

[122] Social Sec. Admin. Baltimore Fed. Credit Union v. United States, 138 F. Supp. 639, 657 (D. Md. 1956); Delmar Vineyard v. Timmons, 486 S.W.2d 914, 920 (Tenn. App. 1972), *cert. denied* by Tenn. Supreme Court, Nov. 6, 1972. Since an auditor's report may reach a broad range of parties who rely on the auditor's opinion of the fairness of the client's financial statements, the auditor's potential liability may depend on the position of the party seeking damages. The client can base an action against an auditor in contract or tort. Dantzler Lumber & Export Co. v. Columbia Gas. Co., 115 Fla. 541, 156 So. 116, 118 (1934); L. B. Lab., Inc. v. Mitchell, 39 Cal. 2d 56, 244 P.2d 385, 388 (1952). *But see* East Grand Forks v. Steele, 121 Minn. 296, 141 N.W. 181, 182 (1913) (auditor ordinarily liable only for breach of contract not negligence). Although the contract sets forth the scope of the auditor's examination, whether or not the auditor has performed the requested services adequately may be a matter of professional malpractice. *See generally* Annot. 92 A.L.R.3d. 396 (1979).

Malpractice claims subsequent to a completed audit ordinarily arise when either a material mistake surfaces in the business' financial statements or a defalcation is discovered within the client's organization. In determining whether an auditor is liable for mistakes or defalcations, a court will hold the auditor to a higher standard of care than a nonprofessional. *See* Gormley, *Accountant's Professional Liability—A Ten-Year Review*, 29 BUS. LAW. 1205, 1206 (1974) [hereinafter cited as Gormley]. The auditor must exercise a degree of knowledge, skill, and judgement normally possessed by members of the auditing profession. Stanley L. Block, Inc., v. Klein, 45 Misc.2d 1054, 258 N.Y.S.2d 501, 506 (Sup. Ct. 1965); Delmar Vineyard v. Timmons, 486 S.W.2d at 920.

In addition to possible liability to the client, the auditor also may be liable to third parties who have relied on the auditor's report. *See generally* Besser, *supra* note 81; *Contemporary Approach, supra* note 81. Following common law principles requiring privity of contract, many courts have refused to grant relief to parties other than the primary beneficiary of the audit. *See, e.g.*, Stephens Indus., Inc. v. Haskins & Sells, 438 F.2d 357, 359-60 (10th Cir. 1971); Investment Corp. of Fla. v. Buchman, 208 So.2d 291, 295-96 (Fla. Dist. Ct. App. 1968); Ultramares Corp. v. Touche, 255 N.Y. 170, 174 N.E. 441, 444-47 (1931). The modern trend, however, is to make the negligent auditor subject to suits by any member of the class whose reliance on the financial statements is foreseeable. Adams, *Lessening the Legal Liability of Auditors*, 32 BUS. LAW. 1037, 1041 (1977) [hereinafter cited as Adams]; *see, e.g.*, Rusch Factors, Inc. v. Levin, 284 F. Supp. 85, 92-93 (D.R.I. 1968); Shatterproof Glass Corp. v. James, 466 S.W.2d 873, 879 (Tex. Ct. App. 1971); RESTATEMENT (SECOND) OF TORTS § 552 (1977).

Third parties also may proceed against an auditor under federal securities law. *See*

Absent extra-ordinary circumstances that require irregular auditing standards or accounting procedures,[123] an auditor can avoid liability by showing that the audit conformed to Generally Accepted Auditing Standards[124] as promulgated by the AICPA.[125]

Compared with law enforcement officials, users, and manufacturers of computer systems, independent auditors are in the best position to contribute to the prevention and detection of computer crime. The AICPA requires auditors to maintain a technical proficiency in the computer area.[126] By reviewing the client's system of internal control the auditor becomes familiar with the client's use of electronic data process-

---

*generally* Gormley, *supra*, at 1216-22. In Escott v. BarChris Constr. Corp., 283 F. Supp. 643 (S.D.N.Y. 1968), the court held an accounting firm liable under § 11 of the Securities Act of 1933, 15 U.S.C. § 77k (1976), for material misstatements in the client's financial statements. 283 F. Supp. at 703. Section 11 provides that auditors or other experts who contribute to the compilation of registration statements may be liable for material misstatements contained in the statements, irrespective of any privity between the auditor and the plaintiff. 15 U.S.C. § 77k(a) (1976). The auditor may assert his due diligence in performing the audit as a defense to a § 11 claim. 15 U.S.C. § 77k(b)(3)(B) (1976). The extent of the auditors due diligence depends upon his adherence to Generally Accepted Auditing Standards. Escott v. BarChris Const. Corp., 283 F. Supp. at 703.

In addition to the statutory cause of action contained in § 11, a third party may have an implied right of action against an auditor under SEC rule 10b-5. Kardon v. National Gypsum Co., 69 F. Supp. 512, 513-14 (E.D. Pa. 1946). Under rule 10b-5 an auditor may be liable for material false statements made in connection with the purchase or sale of any securities. Securities Exchange Act Release No. 3230 (1942). The Supreme Court has held, however, that mere negligence is insufficient to sustain an action under rule 10b-5. Ernst & Ernst v. Hochfelder, 425 U.S. 185, 193 (1976). To impose liability upon an auditor under rule 10b-5, the court must find that the auditor intended to deceive, manipulate, or defraud through the false statement. *Id.*

[123] If an audit requires irregular auditing procedures or a financial statement follows accounting principles that are not generally accepted by the accounting profession, the auditor's report must disclose the irregularities or accounting principles. AICPA Professional Standards AU §§ 509.10, 509.18-.19.

[124] *See Contemporary Approach*, *supra* note 81, at 402 n.10. The Generally Accepted Auditing Standards consist of three general standards, three standards of field work, and four standards of reporting. AICPA Professional Standards AU § 150.02. The AICPA has adopted not only the ten overall standards, but also detailed explanations describing the effect of each standard on the particular audit. *See generally* AICPA Professional Standards AU §§ 200-561.

[125] Hochfelder v. Ernst & Ernst, 503 F.2d 1100, 1108 (7th Cir. 1974), *rev'd on other grounds*, 425 U.S. 185 (1976); *cf.* Rhode Island Hosp. Trust Nat'l Bank v. Swartz, Bresenoff, Yavner & Jacobs, 455 F.2d 847, 852 (4th Cir. 1972) (AICPA standards constitute auditor's minimum duty to client). *But see* United States v. Simon, 425 F.2d 796, 805 (2d Cir. 1969), *cert. denied*, 397 U.S. 1006 (1970). (auditor's criminal liability for conspiracy depends on auditor's good faith); 1136 Tenants' Corp. v. Max Rothenberg & Co., 27 App. Div.2d 830, 277 N.Y.S.2d 996, 997-98 (1967) (accountant held liable for defalcation despite technical adherence to auditing standards), *aff'd*, 21 N.Y.2d 995, 290 N.Y.S.2d 919, 238 N.E.2d 322 (1968). One authority has stated that the auditor's standard of care in an audit involving large computer installations is greater than the standard required by AICPA standards. Bigelow, *supra* note 118, at 10. *See generally Contemporary Approach*, *supra* note 81, at 408 n.43.

[126] *See* text accompanying note 115 *supra*.

ing[127] and the effect that the computer has on the individual client.[128] In addition, because the auditor reviews a number of different operations, he has the ability to compare the security measures employed by different users and provide each client with suggestions on available alternatives. Most importantly, the auditor's complete independence from the organization he is auditing[129] enables the auditor to examine a business' computer system objectively without being subject to the biases and influences of the individual work setting.[130] Thus, the outside auditor has a unique ability to make a major contribution to the prevention of computer crime.

Translation of the auditor's advantageous position into effective computer crime prevention requires placing some of the responsibility for the security of the client's computer system on the auditor. The most effective means of shifting responsibility for computer security to the auditing profession is to require certification of the client's computer security system in every audit.[131] Presumably, AICPA standards for a mandatory review of the client's system of computer security controls would be similar to the standards applied when the client specifically requests a report on the overall system of internal control.[132] Applying these standards would increase auditor responsibility for computer security drastically.[133] Before issuing an opinion on the integrity of the

---

[127] AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, THE AUDITOR'S STUDY AND STUDY AND EVALUATION OF INTERNAL CONTROL IN EDP SYSTEMS 9-13, 15-17 (1977) [hereinafter cited as STUDY AND EVALUATION].

[128] *Id.* at 14-16, 18-20.

[129] AICPA Professional Standards AU § 220.01. The AICPA requires the auditor to be independent not only in fact but in appearance as well. *Id.* at § 220.02. *But see* Roddy, *supra* note 7, at 349 (auditor independence curtailed by necessary reliance on employees of client to operate computer).

[130] *See* note 86 *supra.*

[131] *See* Adams, *supra* note 122, at 1061. The SEC has considered requiring all registered companies to file a certified report on the business' overall system of internal control. *See* SEC Release No. 34-15772 (April 30, 1979) *published in* 17 SEC Docket 421 (May 15, 1979). A proposed SEC rule would require a report stating whether the system of internal control provides reasonable assurances against unauthorized dispositions of assets and inaccurate financial reports. *Id.* at 421-22. The rule would also require disclosure of any material weaknesses in the system of internal control. *Id.* at 421. Moreover, an independent public accountant would have to examine and report on the statement on the system of internal control for the SEC to accept the statement. *Id.* at 422.

The SEC withdrew the proposed rule on June 6, 1980. *See* SEC Accounting Release No. 278, SEC ACCOUNTING RULES (CCH) ¶ 3282. The SEC based the decision to withdraw the rule on a desire to see voluntary action in the private sector toward reporting on internal control. *Id.* at 3802. The SEC plans to monitor voluntary efforts for three years and defer further action until that time. *Id.* at 3802-03. In the event that the monitoring program indicates that voluntary efforts are inadequate, the SEC stated that future regulatory action is a possibility. *Id.* at 3803. Regardless of eventual regulatory action, the SEC recommended that companies which must file with the SEC include audited reports on internal control with other financial statements. *Id.* at 3817.

[132] *See generally* SAS 30, *supra* note 121.

[133] *See* SEC Accounting Release No. 278, SEC ACCOUNTING RULES (CCH) ¶ 3282 at 3816.

client's system of controls over computer operations, AICPA standards would require the auditors to make a detailed review of the design of the system of controls[134] and to test the client's compliance with existing procedures.[135] The auditor's review of the design of the security system would include a determination of whether the client has identified points in the operation of the computer which are vulnerable to abuse.[136] Where vulnerable points exist, the auditor would determine whether the user has adopted procedures designed to prevent abuses.[137] The standard opinion that the AICPA recommends the auditor should issue following an examination[138] would state that the client's system of computer control is sufficient to reasonably safeguard assets from loss.[139] If a material weakness exists in the system of controls, the auditor must disclose that weakness in his opinion.[140]

Despite the thoroughness that the AICPA requires of an auditor before he can certify his client's system of computer security, mandatory certification would not force the auditor to adopt significantly different auditing procedures than procedures currently required in an audit. The standards that the auditor would use to certify a client's system of computer security are very similar to the standards that govern the auditor's review of the client's system of internal control in a regular audit.[141] The major difference is that the former situation requires the auditor to express an opinion on the overall effectiveness of the controls and disclose weaknesses while the latter situation serves only to determine the extent of testing required by the audit.[142] Mandatory certification of computer security as part of every audit would make the auditor's liability for subsequently discovered computer fraud hinge upon the auditor's adherence to standards designed to pinpoint deficiencies in computer security,[143] rather than standards directed to maximizing the overall quality of the financial statements.[144] Thus, requiring computer security certification would place responsibility for the identification of computer crime opportunities on the group best able to perform the task and recommend remedies. Moreover, the auditor's re-

[134] SAS 30, *supra* note 121, at 7.

[135] *Id.* at 10.

[136] *Id.* at 8.

[137] *Id.* at 8-9.

[138] The auditor should issue a standard opinion only if the examination discovers no material weaknesses in the client's system of internal control. *Id.* at 14. If the auditor finds a material weakness, the opinion would describe the weakness, the cause of the weakness, and the type of errors or irregularities that could result from the weakness. *Id.*

[139] *Id.* at 13-14.

[140] *Id.* at 14; see note 138 *supra.*

[141] *Compare* text accompanying notes 132-37 *supra with* text accompanying notes 113-21 *supra.*

[142] *Compare* SAS 30, *supra* note 121, at 10-15 with AICPA Professional Standards AU § 320.01.

[143] *See* text accompanying notes 134-140 *supra.*

[144] *See* text accompanying note 120 *supra.*

quisite familiarity with the client's system of internal control,[145] coupled with the auditor's existing responsibilities for reviewing the system under current AICPA standards,[146] would facilitate the shift of responsibility to the auditing profession.[147] Traditionally, however, only the AICPA has promulgated additional requirements for auditors.[148] The AICPA's enthusiasm for increasing the potential liability of its members is doubtful.[149]

In the absence of voluntary action on the part of the accounting profession, the government's options for increasing auditor responsibility for computer security are limited. Ordinarily, the federal government has declined to mandate auditing standards.[150] In some instances, the Securities and Exchange Commission (SEC) has required auditors and accountants to apply different standards to financial statements and reports filed with the SEC than the standards required by the AICPA or Financial Accounting Standards Board for certification.[151] Attempts to regulate the accounting profession through the SEC have, however, one major deficiency. SEC regulations apply only to businesses that must file with the SEC.[152] Thus, a regulation requiring that an auditor certify the security of a client's security system would apply only to relatively large, public corporations.[153]

While the auditor's contribution to prevention and detection of computer crime consists of identification of potential problems and recommendation of solutions, the conceivable contribution to crime reporting is more direct. Although auditors are in a position to discover computer crimes,[154] auditors normally do not report the incidents to law enforcement officials. The independent auditor's reluctance to report detected crimes stems from a perceived ethical conflict between reporting a discovery to law enforcement officials and simply allowing the client to

---

[145] *See* text accompanying note 114 *supra*.

[146] *See* text accompanying notes 127-28.

[147] *See* text accompanying notes 126-30.

[148] J. CAREY, THE RISE OF THE ACCOUNTING PROFESSION TO RESPONSIBILITY AND AUTHORITY 145-46 (1970) [hereinafter cited as CAREY]. *But see* note 131 *supra*.

[149] The AICPA recently adopted a new auditing requirement relating to the auditor's review of the client's system of internal control. Effective December 24, 1977, auditors are required to report to the client any material weaknesses in the client's system of internal control. AICPA Professional Standards AU § 323.01. The requirement applies, however, only to weaknesses that come to the auditor's attention during the course of the examination. *Id.* Thus, the requirements do not require the auditor to give an opinion on the overall quality of the client's system of internal control.

[150] *See* CAREY, *supra* note 148, at 146.

[151] *E.g.*, S.E.C. Accounting Release No. 261, SEC ACCOUNTING RULES (CCH) ¶ 3265 (accounting changes by oil and gas producers); *cf.* FASB Stmt. No. 19; AICPA Professional Standards AC § 6021 (1977) (accounting standards for oil and gas producers).

[152] *See* note 81 *supra*.

[153] *See id.*

[154] *See 1978 Hearings*, *supra* note 24, at 46 (remarks of Senator Biden).

handle the situation.[155] A statutory requirement that auditors report uncovered computer crime would relieve the auditor of the difficult decision of whether or not disclosure is necessary and would provide further deterrence to the potential criminal. Furthermore, the considerations that mitigate against requiring a user to report computer crimes are not present in the auditor's case.[156] Although requiring management to report crimes could breed devisiveness within the business, crime disclosure does not compromise the auditor's position as an independent, external examiner. Also, since the auditor ordinarily will not benefit from failing to disclose a crime, a mandatory reporting requirement is likely to increase computer crime reporting. Mandatory reporting requirements, however, would constitute unprecedented government regulation of the auditing profession.[157]

In order for the FCSPA to make a significant contribution to the control of computer crime substantial revisions are necessary. The current form of the FCSPA does not encourage increased prevention, detection, and reporting of computer crime.[158] To remedy the deficiencies of the FCSPA, Congress should consider measures directed at those groups that can have the greatest deterrent effect on computer crime.[159] Congress also could adopt a course of action designed to inform computer users of the computer's potential for crime and the punishment that computer criminals can expect upon conviction.[160] Another legislative possibility is a requirement that users and auditors report detected computer improprieties to the proper authorities.[161] Legislation could also provide economic incentives to computer manufacturers to lessen the

---

[155] *1978 Hearings*, *supra* note 24, at 46-47 (remarks of Deputy Assistant Attorney General Keeney); Volgyes, *supra* note 2, at 394.

[156] *See* text accompanying note 95 *supra*.

[157] *See* text accompanying note 150 *supra*; Moss, *The Crisis of Corporate Accountability: A Legislator's View*, 3 J. OF CORP. L. 251, 264-65 (1978) (government promulgation of auditing standards unlikely). A recent 6th Circuit case suggests that judicially created reporting requirements are unlikely. In Adams v. Standard Knitting Mills, Inc., 623 F.2d 422 (6th Cir.) *cert denied sub nom.* Adams v. Peat, Marwick, Mitchell, & Co., No. 80-659 (49 U.S.L.W. 3443, Dec. 15, 1980), a group of shareholders that had relied on an audited proxy statement sought damages from the auditors that had certified the statement. *Id.* at 425. One ground of the plaintiffs' claim stated that the auditors had failed to disclose material weaknesses in the company's system of computer security controls. *Id.* at 431. The 6th Circuit reversed a trial court holding that the auditor's failure to disclose the weaknesses constituted fraud and, thus, the auditors should be held liable for damages caused by the fraud. *Id.* at 431. The circuit court reasoned that since Generally Accepted Auditing Standards did not require disclosure of material weaknesses to parties outside the company, the auditors had no duty to disclose the weaknesses. *Id.* at 431-32; *see* note 149 *supra*. The *Standard Knitting Mills* opinion indicates that courts will be hesitant to require auditors to report client shortcomings in the absence of professional standards or legislative mandates.

[158] *See* text accompanying notes 66-76 *supra*.

[159] *See* text accompanying notes 77-81 *supra*.

[160] *See* text accompanying notes 89-92 *supra*.

[161] *See* text accompanying notes 93-96 & 154-57 *supra*.

gap between data processing technology and security technology.[162] Finally, Congress could exert pressure on the auditing profession to adopt standards that shift some legal responsibility to auditors for the overall integrity of an audit client's system of computer security.[163] By enacting measures specifically directed at deterring computer crime, Congress can begin to control a problem that will become increasingly serious as computer use spreads.[164]

ROBERT M. COUCH

[162] *See* text accompanying notes 106-07 *supra.*

[163] *See* text accompanying notes 131-53 *supra.*

[164] *See* note 2 and text accompanying note 3 *supra.*