UIC John Marshall Journal of Information Technology & Privacy Law

Volume 10
Issue 1 *Computer/Law Journal - Winter 1990*

Article 3

Winter 1990

Computer Crime and the Computer Fraud and Abuse Act of 1986, 10 Computer L.J. 71 (1990)

Christopher D. Chen

COMPUTER CRIME AND THE COMPUTER FRAUD AND ABUSE ACT OF 1986†

FOREWORD

Since this Note was written, three people have been convicted under the Computer Fraud and Abuse Act.* The first was sentenced to nine months in prison and fined $10,000, and the second pleaded guilty without a trial.** The third, Robert Morris, was tried before a jury and found guilty of violating the Act, but still awaits sentencing; he is the first person to be convicted by jury under the Act.***

INTRODUCTION

Computer crime is one of the most intriguing and least understood crimes. The scope of computer crime includes not only new computer-specific crimes, but a multitude of other older crimes as well. Because of the constant change and advances in computer technology, computer criminals will find new and innovative ways to commit existing crimes, in addition to committing crimes that are, as of yet, undiscovered and/or undefined. To meet this evolving class of crime, legislators have enacted several computer crime laws to confront computer felons. Their efforts, however, have not, and will not, suffice to solve the problem of computer crime.

This Note begins by providing a general background of computer crime, including a definition of computer crime, descriptions of the type of people involved with computer crime, the cost and pervasiveness of computer crime, and the measures taken to prevent computer crime. The next section addresses the provisions and shortcomings of the Com-

---

† This Note was awarded Third Place in the Sixth Annual Computer Law Writing Competition (1989).

* *See* Markoff, *Computer Intruder is Found Guilty*, N.Y. Times, Jan. 23, 1990, at A21, col. 1.

** *See* Alexander, *Prison Term for First U.S. Hacker-Law Convict*, COMPUTERWORLD, Feb. 20, 1989, at 1; Markoff, *supra* note *.

*** *See* Markoff, *supra* note *; *Student Guilty in Computer Break-in*, Wash. Post, Jan. 23, 1990, at A16, col. 1; Markoff, *From Hacker to Symbol*, N.Y. Times, Jan. 24, 1990, at A19, col. 1; Burgess, *Guilty Verdict may Slow Hill on "Virus" Bill*, Wash. Post, Jan. 24, 1990, at A11, col. 1; Kates, *Changes Advocated in Computer Law*, L.A. Daily J., Jan. 24, 1990, § I, at 26, col. 2.

puter Fraud & Abuse Act of 1986 and offers some recommendations that could resolve those shortcomings. In addition, problems which are not generally related to computer crime statutes, but which, nevertheless, reduce their effectiveness, are also discussed. The last section suggests an alternative solution to combatting computer crime.

I. BACKGROUND ON COMPUTER CRIME

A. DEFINITION

The first and most basic difficulty with computer crime is the lack of consensus as to what constitutes a computer crime.[1] Judges, lawyers, legislators, and experts in the computer crime field, have struggled, without success, to come up with a definition that adequately describes computer crime.[2] There are several inherent problems with not having a widely accepted and agreed upon definition of computer crime. First, if we do not know what a computer crime is, how can we tell when one has occurred? Moreover, how can we develop effective and consistent solutions to the computer crime problem if computer crime remains undefined? Finally, absent a consensus as to what constitutes computer crime, studies on the subject will continue to produce inconsistent results and conclusions.[3]

In attempting to define computer crime, some scholars have resorted to classifying the *possible* relationships that may exist between computers and crime. For example, Donn Parker, in conjunction with the Stanford Research Institute, listed four roles that computers can

---

1. *Federal Computer Systems Protection Act: Hearing on H.R. 3970 Before the Subcomm. on Civil and Constitutional Rights*, 97th Cong., 2d Sess. 22 (1982) (statement of Milton Wessel, Esq., Parker, Chapin, Flattau & Klimpl, New York); *see also* Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMPUTER/L.J. 353, 363 (1980); BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 3 (1979) [hereinafter RESOURCE MANUAL]; D. PARKER, FIGHTING COMPUTER CRIME 23 (1983).

2. The following definitions illustrate the difference in opinion as to what constitutes computer crime. RESOURCE MANUAL, *supra* note 1, at 3 ("any illegal act for which knowledge of computer technology is essential for successful prosecution"); A. BEQUAI, COMPUTER CRIME 4 (1978) ("the use of a computer to perpetrate acts of deceit, concealment and guile that have as their objective the obtaining of property, money, services, and political and business advantages"); Taber, *A Survey of Computer Crime Studies*, 2 COMPUTER/L.J. 275, 298 (1980) (Taber defines a genuine computer crime as "a crime that, in fact, occurred and in which a computer was directly and significantly instrumental").

3. However, the problem does not end with these inconsistent results and conclusions. Rather, it is compounded by the fact that legislation meant to deal with computer crime is also based on these studies and, consequently, has proven to be ill-suited to properly deal with the problem. *See generally* Taber, *supra* note 2 (discussing the inconsistencies and flaws in several leading computer crime studies).

play in a crime: object, subject, instrument, and symbol.[4] Experts in the field have also classified the methods used in committing computer crimes. Most of these experts have recognized twelve commonly used methods.[5] These methods have names that sound more like something from a computer game than a computer crime. A few examples are: salami techniques, superzapping, logic bombs, piggybacking,[6] data diddling, and trap doors.

Many people who have written about computer crime have avoided the problem of developing a definition by arguing that computer crime is just traditional crime committed in new ways.[7] Although this may generally be true for many computer crimes, some aspects of computer crime are unique, making it very difficult to classify them using traditional crime definitions.[8]

B. THE COMPUTER CRIMINAL

Most computer criminals are relatively young and very intelligent.[9] One study found that the typical computer criminal was between eighteen and thirty years of age.[10] In addition, most of these computer criminals, or "hackers,"[11] have spent an inordinate amount of their time playing with computers and have extraordinary skills and expertise in

4. D. PARKER, *supra* note 1, at 17; *see also* I. SLOAN, THE COMPUTER AND THE LAW 3 (1984).

5. *See* D. PARKER, *supra* note 1, at 75-100 (for a description and examples of the twelve techniques used in computer crimes). *See also* RESOURCE MANUAL *supra* note 1, at 9-29; Reimer, *Judicial and Legislative Responses to Computer Crimes*, 53 INS. COUNS. J. 406, 407-09 (1986).

6. This technique has played a major role in drawing attention to the problem of computer crime. "Piggybacking" is used to surreptitiously send computer "viruses" through communication lines to infect other computer systems, sometimes causing enormous amounts of damage in lost data, computer time, and in the time and effort expended in trying to combat these programs.

7. Reimer, *supra* note 5, at 406 (his definition summarizes this approach: "Computer crimes are not new crimes, they are the same old crimes committed in fresh and inventive ways made possible by the high technology of today's computers and telecommunications."). *See also* Ingraham, *On Charging Computer Crime*, 2 COMPUTER/L.J. 429, 438 (1980) ("Most computer-related crimes are, at their core, the same crimes that have been prosecuted since the apple was plucked and Cain was banished.").

8. *See* Hollinger & Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 103 (1988) (citing D. PARKER, CRIME BY COMPUTER 19 (1976)) (computers as "subjects" in computer crime presents new and unique legal questions).

9. Sokolik, *supra* note 1, at 366. *See* D. PARKER, *supra* note 1, at 103-88.

10. Volgyes, *The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review*, 2 COMPUTER/L.J. 385, 393 (1980).

11. A "hacker" is a term used to describe one who is preoccupied with computers. Hackers spend the majority of their time trying to gain unauthorized access to networks and computer systems, as well as engaging in other forms of computer abuse.

the computer field. Consequently, many of them do not find their jobs to be challenging and end up committing computer crimes at work to avoid boredom.[12] There is a notion that most computer felons do not commit crimes for personal gain, but rather for the sake of a challenge.[13] This, together with the fact that most computer criminals are very young, makes it more difficult to view these people as criminals.

C. COST & PERVASIVENESS

How much computer crime exists? How much does it cost the industry? Based, in part, on the lack of a consistent definition, studies done on the pervasiveness and costs of computer crime have produced inconsistent results.[14] Annual losses due to computer crime have been estimated at $2 million[15] to $730 million,[16] with an average loss per incident ranging from $44,000[17] to $10 million.[18] Another study, done by Stanford Research Institute (SRI), estimated the annual loss at $300 million with an average loss of $450,000 per incident.[19] However, the SRI study, like others, has serious flaws which have led to misleading figures.[20]

According to the 'tip of the iceberg' theory on computer crime detection and reporting, estimates of the costs of computer crime are greatly distorted.[21] Specifically, the author of this theory hypothesizes that the number of computer crimes detected represents only a fraction of the ones actually committed because of the unique characteristics of these crimes. In addition, many researchers believe that most computer crimes go unreported because of fears held by the computer user or

---

12. Volgyes, *supra* note 10, at 393.

13. Sokolik, *supra* note 1, at 367-68.

14. *See generally* Taber, *supra* note 2.

15. *Id.* (citing GENERAL ACCOUNTING OFFICE, COMPUTER-RELATED CRIMES IN FEDERAL PROGRAMS (1976)) (the actual figure arrived at ($2,151,413) represents losses from computer-related crime in federal programs).

16. TASK FORCE ON COMPUTER CRIME, CRIM. JUSTICE SECTION, AM. BAR ASS'N, REPORT ON COMPUTER CRIME 38 (1984) [hereinafter ABA REPORT]. Another commonly quoted figure, especially in computer security advertisements, is an annual loss as high as $3 billion. *See, e.g., Absolute Security Inc. Advertisement*, COMPUTERWORLD FOCUS: COMPUTER SECURITY, June 3, 1987, at 35 (the advertisement claims that "[t]he annual cost of . . . computer crime to business is $3 billion").

17. Taber, *supra* note 2, at 282 (citing GENERAL ACCOUNTING OFFICE, COMPUTER-RELATED CRIMES IN FEDERAL PROGRAMS (1976)).

18. ABA REPORT, *supra* note 16, at 38 (the survey states that reported losses fall "in the range of $2 million to over $10 million").

19. Taber, *supra* note 2, at 288.

20. *See generally id.*

21. Sokolik, *supra* note 1, at 359.

manufacturer.[22] Several studies have estimated that only 1% of all computer crime is even detected.[23] The Federal Bureau of Investigation (F.B.I.) estimates that, of those that are detected, only 14% are actually reported.[24] F.B.I. statistics also estimate that only one in 22,000 computer criminals go to jail.[25]

D. PREVENTION

Two basic approaches have been taken to fight computer crime: legislation and security. In the late 1970's, Florida[26] and Arizona[27] became the first states to enact specific computer crime legislation.[28] In just over ten years, the number of states that have enacted computer crime statutes has grown to forty-eight.[29] On the federal level, Congress has responded by enacting the Counterfeit Access Device and Computer Fraud and Abuse Act in 1984[30] and amending it with the Computer Fraud and Abuse Act in 1986.[31]

Apart from specific computer crime legislation, several other statutes exist which may be used by law enforcement agencies to prosecute computer crimes. There are forty federal statutes[32] and eleven areas of

---

22. *Id.* Some of the fears noted are a loss in public confidence and possible liability for lack of prevention and recovery losses. *Id.*

23. A. BEQUAI, *supra* note 2, at 4.

24. J. BECKER, U.S. DEP'T OF JUSTICE, THE INVESTIGATION OF COMPUTER CRIME 6 (1980) [hereinafter INVESTIGATION]. *See also* T. SCHABECK, COMPUTER CRIME INVESTIGATION MANUAL 1, 4 (1979) (only 15% of computer crime is detected).

25. INVESTIGATION, *supra* note 24, at 6; *see also Federal Computer Systems Protection Act: Hearing on H.R. 3970 Before the Subcomm. on Civil and Constitutional Rights*, 97th Cong., 2d Sess. 22 (1982) (statement of Milton Wessel, Esq., Parker, Chapin, Flattau & Klimpl, New York) (about the FBI estimates: "One finds little source support for such guesses").

26. FLA. STAT. § 815.02 (1983).

27. ARIZ. REV. STAT. ANN. § 13-2301 (1983).

28. *See generally* Gemignani, *Computer Crime: The Law in '80*, 13 IND. L. REV. 681, 695-97, 710-12 (1980) (discussing Arizona and Florida legislation); *see also* M. SCOTT, COMPUTER LAW § 8.17 (1984).

29. *Invasion of the Data Snatchers*, TIME, Sept. 26, 1988, at 67.

30. Pub. L. No. 98-473, § 2102(a), 98 Stat. 1837, 2190 (codified at 18 U.S.C.A. § 1030 (West Supp. 1989)). *See generally* Tompkins & Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem*, 2 COMPUTER/L.J. 459 (1980) (discussing the provisions and shortcomings of the statute).

31. Pub. L. No. 99-474, § 2, 100 Stat. 1213 (amending 18 U.S.C.A. § 1030 (West Supp. 1989)).

32. *Federal Computer Systems Protection Act: Hearing on S. 1766 Before the Subcomm. on Criminal Laws & Procedures of the Senate Comm. of the Judiciary*, 95th Cong., 2d Sess. 6 (1978) (statement of Sen. Abraham Ribicoff); *see also* Nycum, *The Criminal Law Aspects of Computer Abuse: Part II - Federal Criminal Code*, 5 RUTGERS J. COMPUTERS & L. 297, 305-22 (1976) (documenting the forty existing federal statutes under Title 18 of the United States Code that can be used on computer-related crimes). *See generally* Coolley, *RICO: Modern Weaponry Against Software Pirates*, 2 COMPUTER/L.J.

traditional state law[33] that can be used to attack computer crime. The areas of state law include: arson, burglary, embezzlement, larceny, criminal mischief, extortion, forgery, theft, receipt of stolen property, theft of services or labor under false pretenses, and theft of trade secrets.[34] Although this alternative legislation can be used to prosecute computer crimes, it is often difficult to apply traditional laws developed before the computer age, to computer crimes.[35]

The other commonly used method of fighting computer crime is security.[36] The number of companies offering and specializing in computer security has increased dramatically over the past few years. Accompanying this explosion in the security industry has been an expansion in the different types of security offered. A few of the security measures presently available include: retinal patterns, fingerprints, encryption, special keys, and, of course, passwords.[37] Despite a heightened awareness of the need for computer security, many believe that security measures continue to fall short of what is required.[38] One factor which may account for this is the cost involved in providing these security measures.[39] This cost will play an increasing role in the user's security decisions as computer crime and the costs of computer security continue to rise.

II. THE COMPUTER FRAUD AND ABUSE ACT

A. PROVISIONS

On October 12, 1984, President Reagan signed into law the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (the

143 (1980) (discussing the applicability of RICO (Racketeer Influenced and Corrupt Organizations Act) to combat software pirating).

33. Starkman, *Computer Crime: The Federal vs. State Approach to Solving the Problem*, 65 MICH. B.J. 314, 316 (1986).

34. *See* A. BEQUAI, *supra* note 2, at 25-35; Reimer, *supra* note 5, at 407-09 (explaining different computer crime techniques and how they can be prosecuted under existing areas of state law).

35. *See generally* Becker, *The Trial of a Computer Crime*, 2 COMPUTER/L.J. 441 (1980) (noting some of the problems of trying to apply traditional criminal statutes to computer-related crimes); *see also* Volgyes, *supra* note 10, at 395-96; Starkman, *supra* note 33, at 315 (using case analysis of United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978) to demonstrate inherent problems with attempting to apply traditional criminal statutes to computer crime).

36. *See generally* Sokolik, *supra* note 1, at 368-71 (discussing the use of computer security as a method of crime deterrence).

37. *See generally* Tucker, *Security in the First Degree*, COMPUTERWORLD FOCUS: COMPUTER SECURITY, June 3, 1987, at 17-19 (discussing existing and new techniques used in computer security).

38. *See* Sokolik, *supra* note 1, at 371.

39. *See, e.g.*, Tucker, *supra* note 37, at 19 (one security system which uses the pattern of blood vessels in the individual's retina costs between $6,000 and $7,000).

"1984 Act") as part of the Comprehensive Crime Control Act of 1984.[40] This statute became the first piece of legislation specifically targeted at deterring and punishing computer crimes at the federal level. The 1984 Act was amended with the Computer Fraud and Abuse Act of 1986 (the "1986 Amendment").[41] The 1986 Amendment extended the scope of the 1984 Act and clarified some of the ambiguities in the original piece of legislation. The 1984 Act, as extended by the 1986 Amendment, will be referred to as the "Act."

The Act prohibits six types of computer abuse and provides for three types of felonies. The first section of the Act makes it a felony to knowingly access a computer: (i) without authorization or in excess of authorized access, and (ii) obtain information related to national defense, foreign relations, or restricted by Section 11 of the Atomic Energy Act of 1954, (iii) with an intent or reason to believe that it will be used to harm the United States or to help a foreign nation.[42] This crime is punishable by fine, ten years in jail, or both, for the first offense,[43] and imprisonment for up to twenty years for repeat offenders.[44] Subsection 4, added by the 1986 amendment, makes it a felony to knowingly and with intent to defraud, access a federal interest computer and obtain anything of value.[45] Mere use of a computer is not included.[46] This crime is punishable by fine, imprisonment for five years, or both, for first time offenders,[47] and imprisonment for ten years for repeat offenders.[48] Subsection 5, also added by the 1986 amendment, makes it a felony to alter, damage, and destroy information in any federal interest computer if losses surpass $1000, during a one-year period, or if such action interferes with any medical care of one or more individuals.[49] This crime carries with it the same penalties as those outlined in subsection 4.[50]

There are three misdemeanors included in the Act. Subsection 2 of the Act prohibits unauthorized access to obtain information contained in a financial record of a financial institution.[51] A violation of this sub-

40. 18 U.S.C. § 1030 (Supp. III 1985).

41. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213 (1986) (amending 18 U.S.C. § 1030 (Supp. III 1985)).

42. 18 U.S.C.A. § 1030(a)(1) (West Supp. 1989); *see* Atomic Energy Act of 1954, 42 U.S.C.A. § 2014(y) (West 1973).

43. 18 U.S.C.A. § 1030(c)(1)(A) (West Supp. 1989).

44. *Id.* § 1030(c)(1)(B).

45. *Id.* § 1030(a)(4).

46. *Id.*

47. *Id.* § 1030(c)(3)(A).

48. *Id.* § 1030(c)(3)(B).

49. *Id.* § 1030(a)(5).

50. *Id.* § 1030(c)(3)(A), (c)(3)(B).

51. *Id.* § 1030(a)(2).

section is punishable by a one-year sentence, a fine, or both,[52] and a ten-year sentence for repeat offenders.[53] Subsection 3 of the Act prohibits access to any computer that is exclusively for government use. If the computer is only partially used by the government, then subsection 3 prohibits access when such conduct affects the government's use of such computer.[54] The penalties for violating subsection 3 are the same as those for violating subsection 2.[55] Subsection 6 makes it a misdemeanor to traffic passwords or similar access information if it affects interstate or foreign commerce or if the computer is used by the government of the United States.[56] The penalties for violating subsection 6 also follow the penalties under subsection 2.[57]

The specific fine provisions in the 1984 Act were repealed by the fine provisions of the Criminal Fine Enforcement Act of 1984.[58] In addition, the Act includes several definitions that the 1984 Act did not include. For instance, the terms "financial record,"[59] "exceeds authorized access,"[60] "financial institution,"[61] "federal interest computer,"[62] and "computer"[63] (which was also defined by the 1984 Act) are defined. The United States Secret Service is charged with primary authority to investigate offenses under the Act.[64] The Act also allows any other agency, that might have authority, to participate, although it does not specify which agencies have the authority.[65] The Act also makes it a crime to attempt to commit any offense under the Act.[66]

---

52. *Id.* § 1030(c)(2)(A).

53. *Id.* § 1030(c)(2)(B).

54. *Id.* § 1030(a)(3).

55. *Id.* § 1030(c)(2)(A),(c)(2)(B).

56. *Id.* § 1030(a)(6).

57. *Id.* § 1030(c)(2)(A), (c)(2)(B).

58. Note, *Computer Crime*, 24 AM. CRIM. L. REV. 429, 434 (1987); *see also* Criminal Fine Enforcement Act, Pub. L. No. 98-596, 98 Stat. 3134 (1984) (current version codified at scattered sections of 18 U.S.C.A. (West Supp. 1989)). The Criminal Fine Enforcement Act provides for maximum fines ranging from $5,000 to $250,000. 18 U.S.C.A. § 3571(b) (West Supp. 1989).

59. 18 U.S.C.A. § 1030(e)(5) (West Supp. 1989).

60. *Id.* § 1030(e)(6).

61. *Id.* § 1030(e)(4).

62. *Id.* § 1030(e)(2).

63. *Id.* § 1030(e)(1). A computer is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." *Id.*

64. *Id.* § 1030(d).

65. *Id.*

66. *Id.* § 1030(b).

B. PROBLEMS WITH THE ACT

At the time this article was written, in November, 1988, the Act had been in existence for over four years, but had been used successfully in the conviction of only a handful of computer criminals.[67] There are two possible explanations for why the Act has been so ineffective in punishing computer criminals. First, the scope of the provisions of the Act, as well as the language of the Act, make it difficult to obtain a conviction. Second, apart from the Act, computer crime and computer crime laws in general, make it difficult to prosecute under the Act.

1. *Language of the Act*

Congress has done a good job trying to correct a number of the shortcomings in the 1984 Act. However, a few problems with the Act still remain. The first problem involves the scope of the Act. Specifically, the Act focuses primarily on computers used and owned by governmental departments. Yet, computers used and owned by corporate America are arguably subject to the most abuse; yet they are virtually ignored.

Subsections 2 and 6 may be applicable to privately owned business computers, as subsection 2 prohibits access to computers that contain financial records or belong to a financial institution.[68] However, access is not a crime unless information is obtained.[69] The word "obtained" is not defined in the Act. Consequently, the question remains as to whether simply looking at the information is enough or whether the information has to be downloaded to a hard copy.[70]

Subsection 6 prohibits the trafficking of passwords.[71] This, however, is a crime only if it affects interstate commerce.[72] It is unclear exactly what is meant by "affects interstate commerce." Uncertainty about those and other terms may cause prosecutors to steer clear of the Act and, instead, pursue convictions under state laws or other federal statutes.

Another area of computer abuse that is not prohibited by the Act is simple "computer trespass" or browsing, where one breaks into a computer and simply views files or data without actually causing any "harm." For example, if a person breaks into the Pentagon computers

67. As of January 1987, there had been no convictions under the Computer Fraud and Abuse Act. Note, *supra* note 58, at 435 n.46 (statement of Milton Wessel, Professor of Computer Law, Columbia University, Jan. 8, 1987).

68. 18 U.S.C.A. § 1030(a)(2) (West Supp. 1989).

69. *Id.*

70. A "hard copy" is usually a computer printout of data or information stored in a computer's memory.

71. 18 U.S.C.A. § 1030(a)(6) (West Supp. 1989).

72. *Id.*

and just views top secret information, it is not a crime. In order to violate the Act in this case, the person would have to obtain the information with the intent or reason to believe that the information will be used to harm the United States.[73] Under subsection 2, it is not a crime to view financial records as long as no information is obtained.[74] Furthermore, subsection 4 contains an explicit use exception.[75] It allows a person to access a federal interest computer without authorization as long as "the object of the fraud and the thing obtained consists only of *the use* of the computer."[76]

The real danger in allowing this type of computer abuse is that it represents the first step in the commission of computer crime. Although no immediate harm results from computer trespass, if allowed, it will pave the path for future and more severe abuse.[77]

In addition, it would help to clarify the meaning of the statute if terms such as "affect interstate or foreign commerce," "affects the use of the Government's operation," "obtain information," "unauthorized access," and "intentionally access" were defined. Under subsection 3, presumably any access will have at least a minimal affect on the government's use of the computer.[78] How much does one have to "affect interstate commerce" to trigger penalties under subsection 6?[79] Under subsections 1 and 2, if "obtain information" is construed loosely it could encompass merely *looking* at unauthorized data.[80] This interpretation would extend the scope of the Act to include simple computer trespass. Is "unauthorized access" meant to include only unauthorized *direct* access or does it include unauthorized *indirect* access?[81] Furthermore, a literal interpretation of subsection 5 would suggest that if a person unintentionally accesses a computer and then purposely causes over $1000

73. *See id.* § 1030(a)(1).

74. *Id.* § 1030(a)(2).

75. *Id.* § 1030(a)(4).

76. *Id.* (emphasis added).

77. The typical scenario goes something like this: The hacker starts off with a simple challenge such as computer trespass. If this action goes unpunished he will assume that this type of behavior is acceptable. Naturally, as soon as this task is mastered, he will seek a greater challenge, such as altering and destroying data, to satisfy his curiosity and accomplishment. However, if computer abuse is punished at the bottom level—i.e., computer trespass—hackers will be dissuaded from going on to the next and more harmful levels of computer abuse.

78. *See* 18 U.S.C.A. § 1030(a)(3) (West Supp. 1989).

79. *See Id.* § 1030(a)(6).

80. *See Id.* § 1030(a)(1), (a)(2).

81. Unauthorized direct access is where one accesses a computer system absent authorized access at that level. Unauthorized indirect access is where a person has authorized access at the initial level, but then goes on to access another level of the computer system without authorization.

in damage, there would be no penalty.[82] These are but a few examples of the problems generated by the lack of sufficiently clear definitions in the Act.

One last subsection in need of clarification is subsection d which gives the United States Secret Service, "in addition to any other agency," the authority to investigate offenses under the Act.[83] Logically, any other agency would probably mean, among others, the F.B.I. If the Act were to specifically give jurisdiction in such cases, there would be no question as to which agency is responsible for pursuing violations of the Act.[84]

Some of these loopholes in the Act have recently come under scrutiny in light of the damage caused by a computer virus set loose by Cornell University graduate student, Robert Morris.[85] In early November 1988, Morris created a computer virus[86] that took advantage of a bug[87] in a program called *Sendmail*.[88] The virus was sent through the Internet network, a network that links over 60,000 computers at national laboratories, universities, and military installations.[89] It quickly spread across the country and caused many computers to shut down.[90] Luckily, the program did not destroy any data.[91]

Two possible subsections under the Act could be used to prosecute Morris, subsections 3 and 5.[92] Under both of the subsections, the perpe-

---

82. *See* 18 U.S.C.A. § 1030(a)(5) (West Supp. 1989).

83. *Id.* § 1030(d).

84. In the recent computer virus incident involving Robert Morris, the F.B.I. handled the investigation.

85. For a comprehensive description of the developments leading up to the discovery of the computer virus and its aftermath see Wash. Post, Nov. 4-11, 1988, and COMPUTERWORLD, Nov. 7 & Nov. 14 (1988); Alexander, *FBI Expected to Throw Book at Virus Suspect*, COMPUTERWORLD, Feb. 2, 1989, at 2; Alexander, *Morris Indicted in Internet Virus Affair*, COMPUTERWORLD, July 31, 1989, at 8; Alexander, *Not So Fast Please*, COMPUTERWORLD, Aug. 7, 1989, at 37.

86. A "computer virus" is a program which is created for the sole purpose of multiplying and spreading itself to other computers through networking systems that link thousands of computer systems. Sometimes these programs simply multiply and take up space in a computer's memory. Some, unfortunately, actually destroy data in the process. Most viruses are attached to a legitimate program by "piggybacking." *See supra* note 6.

87. A "bug" is a defect in a computer program which can cause the program to operate in a way that it was not intended to. It may be years, however, before the right set of circumstances arise to trigger the bug.

88. Wash. Post, Nov. 7, 1988, at A10, col. 1.

89. *Id.*

90. *See* Alexander, *Virus Ravages Thousands of Systems*, COMPUTERWORLD, Nov. 7, 1988, at 1; Doherty, *Virus Hits Arpanet*, ELEC. ENG'G TIMES, Nov. 7, 1988, at 1; Wash. Post, Nov. 4, 1988, at A1, col. 2.

91. Betts, *Virus' "Benign" Nature Will Make it Difficult to Prosecute*, COMPUTERWORLD, Nov. 14, 1988, at 16.

92. *See* 18 U.S.C.A. § 1030(a)(3), (a)(5) (West Supp. 1989). For a discussion of the ap-

trator must access the computer system intentionally and without authorization.[93] The problem with the Act in relation to this and other computer viruses is that Morris had authorized access at the initial level (the Cornell University computer system).[94] The virus then reproduced itself and spread to other computer systems. Furthermore, friends of Morris claim that he did not intend for the virus to spread so widely nor inflict the damage that ultimately resulted.[95] He claims his intent was to make known a bug in the Sendmail program.[96] Under subsection 5, even if the prosecution proves the intent and unauthorized access, they must prove that the action altered, damaged, or destroyed information.[97] Despite all the problems that resulted, it appears that no such thing happened.[98]

2. *Problems Unrelated to the Act*

The lack of prosecutions under the Act could also be attributed to factors unrelated to the Act. First, the victims of computer crimes are reluctant to report them because the reporting of a computer crime is an admission that the computer system is vulnerable.[99] Victims may fear that the bad publicity will mean a decrease in the confidence level among their clients. Moreover, a simple cost/benefit analysis might convince the victim that the loss in business would not be worth the time and money spent in pursuing the prosecution of the crime.[100]

Another factor which deters victims from reporting computer crimes is their lack of confidence in the system's ability to successfully prosecute the offender. Unfortunately, this concern is not totally unfounded. First, there is a lack of precedent in the computer crime field.[101] From 1978 to 1986, less than 200 computer related prosecutions were initiated on the national level.[102] Therefore, many of the cases being brought are ones of first impression, involving an initial interpretion of a particular computer crime statute. Second, many prosecutors and judges lack the computer knowledge to properly handle computer crime

---

plication of the Computer Fraud and Abuse Act to Robert Morris' actions see Betts, *supra* note 91.

93. *Id.*

94. Wash. Post, Nov. 8, 1988, at A1, col. 2.

95. Alexander, *Security, Ethics Under National Scrutiny*, COMPUTERWORLD, Nov. 14, 1988, at 6; *see also* Betts, *supra* note 91.

96. Wash. Post, Nov. 7, 1988, at A8, col. 1.

97. 18 U.S.C.A. § 1030(a)(5) (West Supp. 1989).

98. Betts, *supra* note 91, at 16.

99. Sokolik, *supra* note 1, at 359; *See also* Stephen, *Law Against Computer Criminals Strengthened*, PC WEEK, Nov. 25, 1986, at 107.

100. Note, *supra* note 58, at 435.

101. Stephen, *supra* note 99, at 107.

102. Hollinger, *supra* note 8, at 117.

cases. Since computer technology is fairly new and constantly evolving, it is very difficult for those who did not grow up with computers to acquire the proper knowledge. We will probably have to wait until a majority of lawyers and judges are familiar and comfortable with computer technology before we see computer crimes properly interpreted and applied.

This lack of computer familiarity leads to many problems, including the problem of how to properly issue search warrants.[103] Lawyers have difficulty in describing exactly what is to be searched.[104] Many times, the thing to be searched does not even exist in physical form but only as bits[105] in the computer's memory banks. The form in which information is stored in a computer also causes trouble for the judge. If the judge issues a search warrant to search the computer files, how can this be done without improperly violating privacy rights?[106] In computer crime cases, judges and lawyers must rely on the expertise of computer experts to help them make decisions at the very start of the criminal proceedings. It is easy to see how the investigation of a simple computer crime could turn sour at its earliest stages.

Once the evidence is obtained, prosecutors face yet another obstacle: the hearsay rule.[107] Computer printouts are usually very crucial to the making of a case, but they are considered hearsay.[108] To get around this rule, prosecutors have tried to admit such evidence as business records.[109] However, this still causes problems because the evidence must have been prepared during the regular course of business in order to fall within this exception.[110] If this course fails, prosecutors may try to admit the evidence under Federal Rule of Evidence 803(24) which allows evidence to be admitted that is material and "is more probative on the point for which it is offered than any other piece of evidence" available.[111]

---

103. *See generally* Becker, *supra* note 35, at 411.

104. *Id.* at 443.

105. A "bit" is a subunit of a byte which is a measurement of memory in a computer. A bit can take on the value of "1" or "0." One character is represented in the computer's memory as a succession of these bits, i.e., "10011101."

106. Becker, *supra* note 35, at 411. For instance, if the judge issues a search warrant for a particular computer, everything in the entire computer might be searched in order to find the relevant evidence.

107. *See* FED. R. EVID. 801-806. *See also* Note, *supra* note 53, at 437-438.

108. Note, *supra* note 53, at 437.

109. *Id. See* FED. R. EVID. 803(6).

110. Note, *supra* note 53, at 437. *See* FED. R. EVID. 803(6) ("A . . . record . . . if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the . . . record [will not be excluded by the hearsay rule]. . . .").

111. Note, *supra* note 58, at 437. *See* FED. R. EVID. 803(24).

III. ALTERNATIVE SOLUTION TO COMPUTER CRIME: EDUCATION

Although Congress has passed the Computer Fraud and Abuse Act and forty-eight states have enacted specific computer crime legislation, the problem of computer crime still exists. There have been very few prosecutions nationwide under any of the computer crime statutes.[112] The proper and more effective solution to computer crime is increased education on four levels. First, and most important, there needs to be more education on computer abuse in the elementary schools all the way up through the universities. Second, users of computer systems need to be educated, and a code of ethics that will foster self-regulation needs to be developed and implemented. Third, the legal community—lawyers, judges, and law enforcement personnel—must be educated on the intricacies of computers and computer crime. Finally, the public must be educated.

The first priority is education in the schools and universities. This is the most important and effective level at which computer crime can be stopped. Children who learn early what is not allowed will carry that knowledge with them to college and eventually into the work force. At least one school district—the Red Bank (New Jersey) school district—has introduced "computer responsibility training."[113] Although this is a step in the right direction, the positive effects of such training will not be fully realized until educators across the entire United States implement such programs.

Institutions of higher learning have been notoriously lenient on computer abusers and, in some cases, have even encouraged such abuse.[114] Many computer science instructors view hacking as a constructive way of learning and developing computer expertise.[115] In response to the Robert Morris incident, Howard McCausland, a computer science professor at Harvard, said: "I realize he's done us all something of a service by calling our attention to a hole."[116] A specific example of a university condoning computer abuse occurred when California Institute of Technology students reportedly received course credit for taking control of a computerized scoreboard during the 1984 Rose Bowl game.[117] Although this example appears harmless, if let go, it could lead to worse computer abuse.

---

112. *See supra* text accompanying note 102.

113. Weintraub, *Teaching Computer Ethics in the Schools*, THE SCHOOL ADMINISTRATOR 8, 9 (Apr. 1986).

114. Hollinger, *supra* note 8, at 113.

115. *Id.*

116. Ryan & Margolis, *Verdict Awaits Monger: Hero or Hacker?*, COMPUTERWORLD, Nov. 14, 1988, at 8.

117. Hollinger, *supra* note 8, at 113.

Leading computer science universities, such as Carnegie Mellon, MIT, and Stanford, should take the initiative by requiring a computer ethics course as part of their computer science curricula. Furthermore, a student code of computer ethics should be implemented and enforced within the major universities. If these steps are taken, it would ensure that students recognize the seriousness of computer abuse and would decrease the probability that those students would engage in computer abuse in the future.[118]

The next area to address is the education of those individuals in the legal field. Very few law schools have courses specifically devoted to computer crime or computer law even though the field of computer law is probably the most rapidly expanding area of the law today and is expected to continue to grow in the future.[119] As previously mentioned, lack of computer literacy among lawyers and judges often prevents effective prosecution of computer criminals.[120] If more lawyers and judges became familiar with computers, the legal system would be better prepared to handle computer crime cases. This, in turn, would increase the public's confidence in the system and encourage victims to come forward with accounts of computer crime.

Education of computer users, such as businesses, corporations, and the government, should begin with the development of a code of ethics. Computer organizations should work with users to develop a code that would be uniformly acceptable. One such organization, the Data Processing Management Association (DPMA), has already developed a model computer crime code. This code, or one similar to it, could be introduced to new employees as part of their training program and discussed in any of the several computer conferences held each year.

At present, there is a wide range of attitudes towards computer crime. Many companies even hire the people who have broken into their systems as security consultants.[121] In response to the recent computer virus ordeal, many have even praised Morris' actions as instructive. *Computerworld* asked individuals at seven companies whether they would hire Robert Morris, two responded that they would.[122] Un-

118. The current attitude about computer abuse in universities is not very promising. A survey of 200 students at a major university indicated that 22% of the students would, definitely or probably, examine or modify confidential information, while only 3% would definitely not. Hollinger, *supra* note 8, at 113.

119. At least two of the leading law schools, Georgetown and Columbia, offer courses in computer law.

120. *See supra* text accompanying notes 101-06.

121. Sokolik, *supra* note 1, at 372.

122. *To Hire or Not To Hire*, COMPUTERWORLD, Nov. 14, 1988, at 8. There has been even more praise of Robert Morris' computer virus by the business community. Peter Neumann, a computer security expert at SRI International, thought that Morris had "done us a great service" and added that he believes Morris will be seen as a folk hero.

til businesses develop a code of ethics which reflects their disapproval of computer crime, computer criminals will continue to perpetrate crimes with their tacit stamp of approval.

A final group which needs to be educated about computer crime is the public. It is very easy for the average person to recognize that murder is wrong. However, because computer crime is often viewed as a "victimless" crime, the average person has difficulty grasping the seriousness of the offense. In this respect, the media will play a major role in educating the public. This will require a departure from the media's past treatment of computer criminals as folk heroes, exemplified by the now famous "414" Gang.[123] One writer has outlined a two pronged role that the media must play in changing the public's attitude towards computer crime.[124] First, the media must convey a sense of the frequency of computer crime, and second, it must convey a sense that computer crime is a threat to society.[125] The media's coverage of the latest computer virus case successfully conveyed the scope and severity of the computer abuse. If the media continues this type of coverage, the public will take a more serious stance on computer crime.

IV. CONCLUSION

Although there are several references in this Note to the "solution for computer crime," very few crimes, including computer crime, can be totally eliminated. However, methods do exist to help curb the alarming rate of computer crime. Specifically, if businesses, the government, the legal system, and educators, couple education with the existing crime statutes, computer crime may be brought under control.

*Christopher D. Chen**

Daly, *Portrait of an Artist as a Young Hacker*, COMPUTERWORLD, Nov. 14, 1988, at 6. Marc Rutenberg, director of the Work Office of Computer Professionals for Social Responsibility commented that: "What happened in this case was not really vandalism, and in many ways I really do think this was a helpful and instructive lesson." Wash. Post, Nov. 8, 1988, at A4, col. 3.

123. BloomBecker, *Computer Crime Update: The View as We Exit 1984*, 7 W. NEW ENG. L.R., 627, 631 (1985).

124. Hollinger, *supra* note 8, at 114-19.

125. *Id.* at 114-15.

* Mr. Chen received a B.S. in Computer Information Systems and Industrial Management, in 1987, from Carnegie Mellon University in Pittsburgh, PA. He is currently a third year law student at Georgetown University, in Washington, D.C., and will begin work as an associate with the Los Angeles office of Mayer, Brown & Platt this Fall.