UIC John Marshall Journal of Information Technology & Privacy Law

Volume 11
Issue 2 *Computer/Law Journal - Spring 1991*

Article 4

Spring 1991

Viewing Computer Crime: Where Does the Systems Error Really Exist?, 11 Computer L.J. 265 (1991)

Darryl C. Wilson

VIEWING COMPUTER CRIME: WHERE DOES THE SYSTEMS ERROR REALLY EXIST?

DARRYL C. WILSON*

I. INTRODUCTION

The new year we ring in heralds the final decade of the Twentieth Century. The media have kept us constantly aware of, if not unduly apprehensive about, the onset of a brave new world filled with dizzying ultra-electronic gadgetry. Visions of Star Trek[1] and the Jetsons, coupled with the latest desires to get back to the future, make one ponder whether the new century will in fact find society lost in space. The common denominator in these seemingly mythical depictions is the computer. Having proliferated into every segment of society, this technological advancement forces reconsideration of whether truth can in fact ever be stranger than fiction.

Computers can truly be characterized as the technological backbone of society; and this new pervasiveness has expanded the traditional category of criminals. Now, the programmer, engineer, and even tape librarian may come under suspicion simply because they have contact with computer terminals.[2] Most of society realizes immediately what "user friendly" encompasses as the computer has become occupationally omnipresent. As such, new guidelines, rules and laws have been developed to assist in maintaining the sanctity of computer usage. However,

* Mr. Wilson, B.B.A., B.F.A., J.D., L..M., is in private practice in Chicago, Illinois, and specializes in general litigation. He is a "hacker" in the truest liberal sense.

1. For a substantial price you can purchase a cellular phone modeled after the Starship Enterprise's ever popular "communicator." Though this item will not allow Scottie to beam you up, you can flip it open, make a long distance call, and then tuck it back into your shirt pocket or utility belt when you are done. Oloroso, *The Search for Six Sigma*, 12 CRAIN'S CHI. BUS. 3 (1989).

2. One wonders how much the shroud of incredulity may encapsulate. While no official studies have been done to comprehensively indicate the boundaries of computer crime perpetrators, monitoring over a twenty-two month period in Detroit indicated that many of the transgressors were under seventeen years of age and involved themselves in activities as mundane as stealing long distance telephone services (phone phreaking). F. HUBAND & R. SHELTON, PROTECTION OF COMPUTER SYSTEMS AND SOFTWARE (1986).

the exponential growth in usage has prompted predictions of a similar growth in crime. In short, many people are finding objectional ways to become more than just friendly users.

II. FORMAT

There has been sweeping legislative response to computer criminal activity throughout the country. Unfortunately, the response has been both extremely slow and of questionable effectiveness. Furthermore, judicial implementation has been irresolute. This paper will focus on possible reasons for the deficiencies in the legal development of this area.

Though both state and federal responses to the proverbial bad apple (with no offense to MacIntosh) will be examined, I will not attempt to individually critique each potentially relevant statute.[3] Instead, I will concentrate on the most pertinent federal legislation[4] and analyze the particular responsiveness of the State of Illinois.

III. DATA EVOLUTION

The definitional aspects of computer law, and therefore computer crime, have historically proven stumbling blocks for those seeking to set

---

3. All states except Arkansas, Vermont and West Virginia have now enacted statutes to combat computer crime. Note, *Computer Viruses and the Law*, 93 DICK. L. REV. 625, 641-42 (1989).

4. As recently as 1986 federal authorities still found themselves groping through nearly forty potentially applicable statutes in attempts to prosecute computer wrongdoers. These included:

18 U.S.C. § 797 (1990): Proscribes publication and sale of photographs or sketches of military equipment and defense installations.

18 U.S.C. § 799 (1990): Establishes standards for security violations of National Aeronautics and Space Administration (NASA) regulations.

18 U.S.C. § 912 (1990): Makes it unlawful to obtain a thing of value by impersonating an officer or employee of the federal government.

18 U.S.C. § 952 (1990): Prohibits the intentional disclosure of diplomatic codes.

18 U.S.C. § 371 (1990): Defines conspiracy; makes it unlawful for two or more persons to conspire to defraud the Federal government.

18 U.S.C. §§ 471-500 (1990): Forgery and counterfeiting statutes; limited applicability in current form.

18 U.S.C. §§ 656, 657 (1989): Makes theft, embezzlement and the like unlawful where the perpetrator is an employee, officer, agent or is connected with a Federally regulated bank or savings and loan association.

18 U.S.C. §§ 1005, 1006 (1989): Proscribes the making of false entries in bank and credit institution records, including omissions, obliterations, and alterations.

18 U.S.C. §§ 1341, 1342 (1989): Makes it unlawful to use the mails for the purpose of executing or attempting a scheme to defraud or to obtain money or property under false pretenses.

I. SLOAN, THE COMPUTER AND THE LAW 71-73 (1984).

forth adequate deterrents. While the computer has been involved in crimes for quite some time, the rapid changes in its practical uses have stymied legal attempts at specifying impropriety.

The current trend is to use the term "computer related crime," thus conveying a broad meaning encompassing any illegal act for which knowledge of computer technology is essential.[5] All computer crimes involve the computer as either the object, the subject, the instrument or the symbol.[6] As with any popular instrumentality, wrongdoing usually can be traced back to a time near its origin. Abuse of computers follows suit, with the earliest documented citings dating to 1958.[7] Initial concerns manifested themselves in the areas of national security, science and engineering.[8] However, with mainstream acceptability of computers came new considerations.

The first computer crime identified as resulting in federal prosecution occurred in Minneapolis in 1966.[9] Later that year, Texas became the first state to grapple with the applicability of common law property concepts to computers. In *Hancock v. State*,[10] a programmer employed by Texas Instruments was ultimately convicted of the theft of fifty-nine computer programs. The trial court found that the programs fit the

---

5. *Id.* at 3.

6. One computer abuse study has set computer crime into five dimensions:

1. Categorized by type of loss: physical damage and destruction from vandalism, intellectual property, direct financial gain and use of services.

2. Categorized by the role played by computers: object of attack, unique environment and forms or assets produced, instrument and symbol.

3. Categorized by type of act relative to data, computer programs, and services: modification, destruction, disclosure, and use of services.

4. Categorized by type of crime: fraud, theft, robbery, larceny, arson, embezzlement, extortion, conspiracy, sabotage and espionage.

5. Categorized by modi operandi: physical attacks, false data entry, superzapping, impersonation, wire tapping, piggybacking, social engineering, scavenging, trojan horse attacks, trap door use, asynchronous attacks, salami techniques, datum leakage, logic bombs, and simulation.

Id. at 6.

7. The United States Justice Department attempted to collect computer crime data from the years 1958 through 1979 and during that time cited 669 computer abuse cases. Ninety-seven involved physical destruction, 185 involved deception and/or taking, 284 involved financial deception and/or taking, and 103 involved the unauthorized use of services. Reimer, *Judicial and Legislative Responses to Computer Crimes*, 53 INS. COUNS. J. 406, 406 (1986).

8. There were sporadic citings of abuse even with the emergence of computers in the late 1940's. During this period, President Franklin Roosevelt instituted the first security classification system in response to perceived national security concerns. Soma & Bedient, *Computer Security and the Protection of Sensitive but not Classified Data: The Computer Security Act of 1987*, 30 A.F. L. REV. 135, 138 (1989).

9. I. SLOAN, *supra* note 4, at 7.

10. 402 S.W.2d 906 (Tax. Crim. App. 1966), *aff'd sub nom.* Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967).

statutory definition of "all writing . . . of every description, provided such property possesses any ascertainable value."[11] *Hancock* might have set the tone for a natural evolution of common law rules concerning property interests in computers. Instead, there began an earnest dispute concerning whether precise language or broad terminology would be most effective in protecting those property interests.

In 1972, a California computer service company employee named Ward used his employer's computer access code to convert a program to his own use. The employee was ultimately charged with theft of a competitor's computer program.[12] The penal code only deemed theft to apply in situations where an article was in fact carried away.[13] Ward had only directed a retransmission of certain electronic impulses through a process known as "on-line" processing. But for Ward having made a printout of these impulses and carrying it away, his motion to dismiss may in fact have been sustained.[14]

These two cases illustrate the base of the controversy. There were no overriding federal directives setting forth what determined the existence of a property interest. The concept of a taking was inadequate to deal with unauthorized access to confidential computer material. The state penal codes defined property in divergent ways, and all levels of government exhibited a total void of law relative to computers.

In 1977, the federal government first attempted to fill this vacuum. The Federal Computer Systems Protection Act[15] (hereinafter FCSPA) was introduced. The bill's introduction stated that the measure was meant to ease the difficulty of prosecution that existed at the time.[16] Congress felt that the best way to do this was by using extremely broad language in the bill's general provisions, proscribing any knowing, willful manipulation or attempted manipulation of a "computer, computer system, computer network or any part thereof . . . ."[17] Hence, the offense actually committed by the computing malfeasant could finally be linked with a truly punitive remedy.[18]

---

11. Hancock v. State, 402 S.W.2d 906, 908 (Tex. Crim. App. 1966).

12. Ward v. Superior Court, 3 Computer L. Serv. Rep. 206 (1972).

13. CAL. PENAL CODE § 499c(b) (West 1970).

14. *Ward*, 3 Computer L. Serv. Rep. at 208.

15. S. 1766, 95th Cong., 2d Sess., 123 CONG. REC. 10,790 (1977). After various hearings before legislative subcommittees, the bill was faced with minor revisions and was reintroduced as S. 240, 96th Cong., 1st Sess. (1979).

16. *Id.* at 10,792.

17. S. 240, 96th Cong., 1st Sess., § 1028(a) (1979).

18. In response to the potentially disastrous economic effect of large scale computer crimes, particularly harsh penalty provisions, including the possibility of jail sentences up to 15 years and fines up to 2 1/2 times the amount of the fraud or theft. *See* Roddy, *The Federal Computer Systems Protection Act*, 7 RUTGERS J. COMPUTERS, TECH. & L. 343 (1980).

However, the FCSPA was not initially enacted, despite the increasing need for some type of legislation. Thereafter, little action was taken to implement the FCSPA; the government's inability to prosecute computer crimes continued. *United States v. Seidlitz*[19] was the next case to punctuate this malady. In 1978, the Maryland defendant used a telephone link to gain access to a former employer's computer, and ultimately obtained a confidential program. Because his point of access was from his office located in Virginia, this offense raised another important issue. Prosecutors charged him with violation of the federal wire fraud statute[20] and with interstate transportation of stolen property.[21] Because only electronic impulses were transferred, the Fourth Circuit refused to interpret the offender's action as falling within the traditional meaning of taking or stealing.[22] The court did find sufficient evidence to let stand a jury finding that the computer system was "property."[23] The defendant was ultimately found guilty under the wire fraud statute, and then, only because his telephone access involved crossing a state line.[24]

Subsequent to *Seidlitz*, federal legislators again attempted to revive the FCSPA.[25] This new version featured a rewording of the definition of a computer to more specifically indicate what activities would be deemed criminal. Provisions also existed, which granted the federal government concurrent jurisdiction with the states, reduced the penalties, and eliminated some of the bill's computer jargon.[26] This revitalized version of the FCSPA likewise failed to be adopted by either the House or Senate.

As a result, state lawmakers decided that they had waited long enough. In 1978, Florida became the first state to pass laws dealing specifically with prohibitions related to computer crime.[27] Illinois was among a group of states to enact similar laws shortly thereafter.[28] No longer would Illinois be forced to rely on antiquated precedent in its attempts to determine whether computers and their accessories fell

19. 589 F.2d 152 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979).

20. 18 U.S.C. § 1343 (1976).

21. 18 U.S.C. § 2314 (1976).

22. *Seidlitz*, 589 F.2d at 155.

23. United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979).

24. *Id.*

25. H.R. 1092, 98th Cong., 1st Sess. (1983).

26. Starkman, *Computer Crime: The Federal v. State Approach*, 65 MICH. B. J. 314, 315 (1986).

27. FLA. STAT. ANN. § 815 (West 1978).

28. ILL. ANN. STAT. ch. 3P, para. 16-9 (Smith-Hurd 1979).

within the definition of property.[29] The Illinois statute also solved the question of valuation which had historically plagued legislators. The issue was whether damages should be figured in light of the (possibly) determinable worth of the intangible information or the tangible value of the item in question.[30]

The Illinois statute defined property broadly enough to encompass both tangible and intangible values. Illinois deemed property as "anything" having value.[31] Though the other states' statutes seemed compatible, an intensified reading indicated a lack of uniformity. Initially, Illinois failed to provide for specific civil remedies and, instead, simply stated "this section shall neither enlarge nor diminish the rights of parties in civil litigation."[32] The penalty provisions were amended in 1984 to include a right of action for civil remedies allowing injunctive relief, reasonable attorney's fees and actual damages under certain circumstances.[33] The law prohibited knowingly gaining access or obtaining the use of a computer system or any part thereof without the owner's consent. Also forbidden was the alteration or destruction of a computer system, its programs, or data without the consent of the owner, as well as using the computer in any fraudulent schemes.[34]

In the meantime, after the numerous above-referenced failed attempts, Congress finally passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (hereinafter the "Act").[35] It is unclear whether it was the years of languishing in Congressional debates or pressure from the Executive Branch itself,[36] but something clearly caused a lack of vision in the Federal Act. The rather myopic promulgations generally established felony penalties for unauthorized access or use of computers in ways that could compromise national se-

29. The Illinois statute addressed property issues, in a separate section. *See* ILL. ANN. STAT. ch. 38, para. 15-1 (Smith-Hurd 1979).

30. This could be a piece of plastic or simply a strip of magnetic tape. Roddy, *supra* note 18, at 359.

31. ILL. ANN. STAT. ch. 3P, paras. 16-9, 15-1 (Smith-Hurd 1979).

32. Reimer, *supra* note 7, at 419.

33. ILL. ANN. STAT. ch. 38, para. 16-9 (Smith-Hurd 1985). The criminal penalty provisions of the act were relatively weak, limiting the sentences to either a petty offense, a Class A misdemeanor, or a Class 4 felony.

34. ILL. ANN. STAT. ch. 38, para. 16-9 (Smith-Hurd 1985).

35. Pub. L. No. 98-473, 98 Stat. 2190 (1984) (codified at 18 U.S.C. § 1030 (1986)).

36. The White House issued a National Security Directive in 1984 establishing procedures for an increased effort to protect sensitive information and for the National Security Agency to take a more definitive role relative to computer and telecommunications security throughout the Federal Government. F. HUBAND & R. SHELTON, *supra* note 2, at 247. *See also* Soma & Bedient, *supra* note 8, at 138-39 (critiquing the "information mosaic theory" of the Reagan administration, wherein the flow of information to the public has been restricted by the conversely expanding concept of national security).

curity.[37] Misdemeanor penalties were established for other intrusions into government computers or into computers containing restricted financial information.[38]

The title of the Act was something of a misnomer. The enacted provisions did not address counterfeit access devices, and were not directly aimed at stopping computer fraud.[39] The Act was important, however, as the first federal statute of its kind. The general provisions attempted to prohibit computer misuse with broad, yet straightforward, directives. The breadth of the terminology later proved inauspicious, notwithstanding the sincere efforts of Congress to avoid both over and under inclusiveness.[40] Congress failed to define key terms or clearly outline the investigative and jurisdictional aspects of the legislation, leaving many calling for amendments to the Act.[41]

Despite its shortcomings, it appeared that the new Act would be an adequate prosecutorial device. Early in 1985, the first indictment under the Act was reported.[42] Later that year, the Act was amended by the Computer Fraud and Abuse Act of 1986.[43]

IV. THE CURRENT PROGRAM

The present status of computer protection on the federal level is three-pronged. The foremost provision is the Computer Fraud and Abuse Act of 1986 (hereinafter "CFAA").[44] The CFAA is the result of a decade of political hacking in search of the proper language necessary to supplement state efforts and fill in particular jurisdictional gaps where the state prosecutions are hampered by complicated extradition procedures. It was noted in a Senate Report, however, that the CFAA was intended to limit federal jurisdiction to situations where a compelling federal interest exists.[45] The CFAA's latest modifications took

37. *See* 18 U.S.C. § 1030(a)(1) (1985).

38. *Id.* § 1030(a)(2), (c).

39. Tompkins & Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem*, 6 COMPUTER/L. J. 459, 462 (1986).

40. For instance the only definition provided for was "computer," while terms such as "access," "USC," and the prohibitive "without authorization" were left undefined. This raised serious jurisdictional concerns. The American Civil Liberties Union attacked the bill for the possibility that it could be used to limit "whistleblowing" activities since federal employees with computer authorization were covered under the Act. Chicago Daily L. Bull., June 4, 1986, at 1, col. 2.

41. Tompkins & Mar, *supra* note 39, at 478-81.

42. United States v. Fadriquela, No. 85-CR-40 (D. Colo. 1985).

43. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030 (1986).

44. *Id.*

45. S. REP. NO. 99-432, 99th Cong., 2d Sess. 4 (1986), *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 2479, 2481-82.

place three years ago and simplified its language while broadening its scope.

The CFAA consists of six sections. These sections respectively prohibit:

(a)(1) - knowing unauthorized access to obtain information deemed restrictive by virtue of Executive Order for national security purposes;

(a)(2) - intentional unauthorized access to financial institution or consumer reporting agency files;

(a)(3) - intentional unauthorized access to any government computer which affects the government's operation of the same;

(a)(4) - knowingly accessing a "Federal interest" computer with the intent to defraud and obtain anything of value in excess of the use of the computer itself;

(a)(5) - intentional unauthorized access of a "Federal interest" computer whereby such conduct alters, damages, destroys information therein, or prevents authorized use; and

(a)(6) - knowingly trafficking passwords or similar information with the intent to defraud provided such trafficking affects interstate/foreign commerce or such computer is used by or for the federal government.[46]

Sections (a)(4) to (a)(6) are part of the recent amendments to the Act.[47] While the CFAA simplified much of the language used by its predecessor, it also failed to define key terms such as "computer" and "access."[48] Further, though the potential exists for an offender to serve a substantial jail term, the Act lacks potency in the area of financial restitution.[49] The CFAA also fails to provide for civil remedies.

The second prong of federally related computer legislation can be found in the Electronic Communications Privacy Act of 1986 (hereinafter "ECPA").[50] The ECPA proscribes the unauthorized interception of

46. Pub. L. No. 99-474, § 2(a)-(c), 100 stat. 1213, 1213-14 (1986). Note the act fails to define a "Federal interest computer."

47. The amendments also changed the wording "or having accessed to a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" to "or exceeds authorized access" in sub-sections (a)(1) and (a)(2). Pub. L. No. 99-474, § 2(a)-(c), 100 Stat. 1213, 1213-14 (codified at 18 U.S.C. § 1030(a)(4)-(6) (1986)).

48. *See supra* note 40 as to terms undefined in the prior Act which still have not been defined by the current statute.

49. 18 U.S.C. § 1030(c) sets forth the penalty provisions of the statute wherein the maximum jail term can be 20 years but the fine referred is only $1,000. Studies in 1986 estimated computer thefts to amount to anywhere from $100 to $300 million a year. Others have stated that the average take for a computer crime offender is $435,000. *See supra* note 25 and accompanying text.

50. 18 U.S.C. §§ 2510-2521 (1987).

an electronic communication.[51] This law was necessary to update what was formally known as the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter "OCCSSA").[52] Because the advent of electronics was not contemplated in OCCSSA's formulation, it soon became outdated, and the ECPA was needed to protect existing and future forms of communication.[53]

Only three of the ECPA's eleven sections can be deemed relevant to computer crime,[54] and the statute never explicitly uses the term "computer" except where including computer facilities as a part of the scope of an "electronic communications system."[55] However, as most occupations entail the use of electronic transmissions, the ECPA can be deemed applicable to any transfer of information from one database to another. The ECPA also covers the activities of a hacker[56] who improperly accesses another's data transmission.

As the ECPA is focused more on electronic communications, this necessarily includes electronic mail, electronic bulletin boards, digitized textual information, and videotext.[57] All of these are computer communications typically found in any office environment. The ECPA provides for substantial damages in its remedy sections.[58] The dollar amounts listed state that a plaintiff in a civil action may receive the greater of $100 a day in statutory damages, up to $10,000, or actual damages.[59] The ECPA also contains a provision for "punitive damages," though these are only to be awarded in "appropriate cases," which the ECPA neglects to define.[60] The potential jail time is limited to five

51. *Id.* § 2511(4)-(5). This unauthorized interception is now considered a crime, as well as an invasion of privacy, possibly subjecting one to civil liabilities and damages.

52. 18 U.S.C. §§ 2510-2520 (1970).

53. Clukey, *The Electronic Communications Privacy Act of 1986: The Impact On Software Communications Technologies*, 2 SOFTWARE L. J. 243, 245 (1988). Actually, the former Act was commonly known as the Wire Fraud Statute and had in fact been used in previous attempts to halt computer crime. *See supra* note 19 and accompanying text.

54. Section 2510 sets forth the definitions used in the ECPA, and section 2511 prohibits interception, usage, disclosure by improper means of any wire, oral or electronic communication. Section 2512 prohibits sending, manufacturing, or advertising devices to be used to intercept electronic communication.

55. 18 U.S.C. § 2510(14) (1987).

56. Not to be confused with your "political hack," the term "hacker" once indicated that one was a computer wizard, or at least particularly adept at programming. It has as of late come to characterize anyone who misuses or illegally uses a computer. R. PERRY, COMPUTER CRIME (1986).

57. Clukey, *supra* note 53, at 251.

58. 18 U.S.C. § 2520 (1987).

59. The "valuation" issue still exists, however. *See supra* notes 28-29 and accompanying text.

60. 18 U.S.C. § 2520(b)(2) (1987).

years.[61]

Like those under the CFAA, prosecutions for computer crimes under the ECPA are almost nonexistent.[62] Although this cannot be linked to narrow security-related terminology like that of the CFAA, it probably is related to the CFAA's existence. The fact is that the CFAA at first glance looks to be the proper source for prosecution if for no other reason than its name. If more civil practitioners are willing to get involved in the area of bringing computer crime cases, the jurisdictional language of the ECPA will definitely cause it to be the statute of choice. With the CFAA's current failure to provide for civil remedies, there is no federal alternative. Yet, there is an alternative where computers and national security are concerned.

The Computer Security Act of 1987[63] (hereinafter "CSA") is the third prong of federal computer-related legislation. Congress obviously felt that the scope of computer usage throughout the government called for more attention than the CFAA could provide.[64] Among the reasons given for this statute's enactment were the overlapping responsibilities given to various agencies relative to security enforcement, increased awareness of security needs, and a lack of clarity regarding what information needed to be secured.[65]

The reasoning behind CSA is somewhat distinct from its purpose, and is generally stated as improving the security and privacy of sensitive information in federal computer systems through improved training. This is achieved by establishing a governmental focal point which, in turn, is responsible for developing security standards and guidelines and requiring agencies to implement security plans.[66] The current gov-

---

61. *Id.* § 2511(4)(a). *See also id.* §§ 2511(5), 2520(c) (wherein under certain circumstances the type of relief available is limited to an injunction and a $500 fine if the injunction is violated).

62. No prosecutions have been cited for computer crime under the ECPA. There was one indictment under the CFAA's predecessor, however. *See supra* note 41 and accompanying text. In *Sawyer v. Dept. of Air Force*, 31 M.S.P.R. 193 (1986), the criminal provision of the CFAA was invoked against an Air Force employee who had altered computer contracts for what he stated was an effort to point out the lack of security safeguards. For a discussion of one of the first cases to be fully prosecuted under the CFAA, see *infra* notes 101-10 and accompanying text.

63. 40 U.S.C. § 759 (1987). CSA provides for procurement, maintenance, operation and utilization of automatic data processing equipment. Though the Code Index cites to this section, the references therein direct one to 15 U.S.C. § 278g-3 entitled "Computer Standards Program" and § 278g-4 entitled "Computer System Security and Privacy Advisory Board" as the Computer Security Act of 1987, by virtue of the provisions of Pub. L. No. 100-235, 101 Stat. 1724 (1987).

64. *See* Soma & Bedient, *supra* note 8, at 135-36 (for a breakdown of statistics related to federal government usage of computers).

65. *Id.*

66. *Id.* at 142.

ernmental focal point is the National Bureau of Standards. The National Security Agency, along with the Department of Defense, is responsible for assuring implementation of these standards.[67] The Computer Security Act of 1987 carries no criminal provisions. Interested parties may be entitled to reasonable attorneys fees and contractual remedies in certain instances involving automated data processing disputes.[68] However, CSA is generally an administrative directive.

You are probably thinking that a three-pronged federal attack would provide more in the way of potential relief for a computer crime than these do. With more than thirty years of data and dire predications for the future,[69] it would seem that the federal government would strive to be the proverbial beacon in the darkness. As this is not to be, where is one to look for an adequate remedy? Once again, the answer is "to the states."[70] Forty-seven states now have computer crime statutes, with Illinois being among the earliest proponents.[71]

The Illinois act, discussed above, was recently amended, changing the look, structure, and feel of the statute. But the act's scope was only slightly altered.[72] The new act has been expanded from four to seven sections. In the primary section, which defines the act's terms, the definitions of "computer," and "computer program" or "program," were expanded.[73] The act also dropped its attempt to demarcate each type of computer-related activity by replacing many former definitions with an expanded concept of property.[74] The language is much simpler and seems to indicate that the amendments were designed to reflect an increased technological understanding on the part of the lawmakers.

Three sections of the act set forth the particular forbidden activities. The first section proscribes "computer tampering," an offense committed when one knowingly and without or in excess of authoriza-

---

67. *Id.* at 166-67.

68. 40 U.S.C. § 759(f)(5) (1987).

69. *See supra* notes 7, 49.

70. *See supra* note 3 (identifying the states who now have specific legislation on computer crime).

71. *See supra* note 28 and accompanying text.

72. ILL. ANN. STAT. ch. 38, para. 160-1 to 160-7 (Smith-Hurd 1989), known as the "Computer Crime Prevention Law," was added by P.A. 85-926, § 1, (Senate Bill 1335) effective Dec. 1, 1987.

73. *Id.* para. 16D-2. "Computer" now means a device that accepts, processes, stores, retrieves or outputs data and includes but is not limited to auxiliary storage and telecommunications devices connected to computers. The former definition said computers meant an internally programmed, general purpose digital device capable of automatically accepting data, processing data and supplying the results of the operation.

74. *Id.* para. 16D-2(d) (wherein the present act expands the definition of property for computer purposes thus eradicating the former perceived need and respective definitions for terms such as "telecommunication," "electronic bulletin board," "identification codes/password system," and "computer network").

tion accesses any part of a computer and obtains data or services, damages the computer, or alters, deletes, or removes data.[75] The second section prohibits "aggravated computer tampering," which is committing the above act or acts, in addition to interfering with vital governmental operations, or creating a strong probability of death or great bodily harm to one or more individuals.[76] The final section condemns the act of "computer fraud," which involves accessing any part of a computer, or obtaining use of the same, where damage is done or a scheme is devised to generally defraud another or to obtain money, control, or property.[77]

Each of the three sections carries its own remedial subsection. Unfortunately, the penalties set forth therein are light, as is the norm with computer statutes.[78] The most troubling aspect is the complete removal of the civil remedies section. This section has been replaced by a truly onerous section providing for the forfeiture of any monies, proceeds, profits, or proprietary interests acquired as a result of committing computer fraud.[79] Although the language of the section is powerful and all encompassing, much like the forfeiture provisions used by federal drug enforcement agencies, the proceeding can only be instituted by the Attorney General or State's Attorney.[80] Though fitted with a rebuttable presumption in favor of the prosecution[81] and a burden of proof of only a preponderance of the evidence, the administrative requirements appear to be much too costly and time consuming to use.

There have been no reported decisions involving the Illinois statute, though states in general are beginning to indicate a willingness to prose-

---

75. *Id.* para. 16D-3.

76. *Id.* para. 16D-4. This language presumably reflects the influence of National Security seen in the federal acts. There is a dearth of legislative commentary on the Act as a whole but no information with respect to when, or how often, death or great bodily harm are serious concerns in computer crime.

77. *Id.* para. 16D-5.

78. The penalty provisions provide for a wide range of findings against an offender. Under paragraph 16D-3 one can be found guilty of a Class A or B misdemeanor, or Class 3 or 4 felony. Under paragraph 16D-4 one can be found guilty of either a Class 2, 3 or 4 felony depending on the value of the property or services involved.

79. ILL. ANN. STAT., ch. 38, para. 16D-6.

80. *Id.*

81. *Id.* para. 16D-7. A rebuttable presumption exists that the computer was accessed without the authority of the owner or in excess of the granted authority whenever a computer is accessed by virtue of a confidential or proprietary code not issued to the offender. *But see* Sawyer v. Dept. of Air Force, 31 M.S.P.R. 193 (1986) (wherein Sawyer argued that he did not intend to defraud the government and it was ruled that the CFAA only requires proof of use for unauthorized purposes to involve its criminal provisions. Neither the CFAA nor any of the federal acts explicitly state that such a presumption in favor of the government exists.).

cute and convict under these types of statutes.[82]

V. TESTING THE SYSTEM

The sections above point out that prosecutors have quite a choice of statutes on the state and federal[83] levels if they are seeking to prosecute computer related activity. However, it is also apparent that few prosecutions are taking place. It may be that much of this type of crime simply goes unreported. The reasons may be related to a cost-benefit analysis of the lawsuit, or a lack of sophistication or resources on the part of companies to fully investigate discovered crimes. Large scale thefts perpetrated through computerized financial transactions call attention to themselves by their sheer magnitude; and because they normally entail the use of federally interested computers, there is no hesitation to prosecute although the prosecution is usually based on some criminal statute.[84] Yet, many of the recent crimes committed do not involve large scale thefts. Indeed, some of the most recent computer crimes involve individuals who, in essence, attack others through the improper usage of the computer. These methods of attack are identified by a number of different names, but basically fit into twelve classifications.[85] Let us examine the prospects for judicial response in

82. *See* People v. Versaggi, 518 N.Y.S.2d 553 (1987) (first prosecuted under New York's Computer Crime Statute; defendant was charged with two counts of computer tampering for entering unauthorized commands into the computer); Mahru v. Superior Court, 191 Cal. App. 3d 545, 237 Cal. Rptr. 298 (1987) (the first prosecution under California's 1979 computer law; petitioner was acquitted even though he caused a shut down of his employer's computer because he was acting within the scope of his employment at the time and third party damage was not determinative in applying the statute); State v. Olson, 47 Wash. App. 514, 735 P.2d 1362 (1987) (Washington court overturned a conviction for computer trespass since the employee was authorized to use the computer in question despite his personal use of the data); State v. Burleson, No. 0324930R (Dist. Ct. Tarrant Cty. Tex. 1988) (an employee was convicted under the Texas statute for injecting a harmful program into a company computer which took effect two days after his firing).

83. Aside from the CFAA, ECPA, and CSA, protections are available under the Copyright and Patent Laws. *See* 17 U.S.C. §§ 101-914 (1989); 35 U.S.C. §§ 101-376 (1989).

84. Roddy, *supra* note 18.

85. The classifications are as follows: (1) *Data Diddling* -involves hanging data before or during their input to computers; (2) *Trojan Horse* - the covert placement of instructions in a computer program that usually allows the intended functions but also performs unauthorized functions; (3) *Salami Techniques* - involves the theft of small amounts from a large number of sources; (4) *Superzapping* - computer stops, bypasses, malfunctions and the utility superzap program provides the universal access allowing the computer to start functioning again; (5) *Trapdoors* - the insertion of debugging materials into a program that provide breaks in the code for the insertion of other code; (6) *Logic Bombs* - a program executed at one time that perpetrates a malicious act under certain circumstances set forth in the original program; (7) *Asynchronous Attacks* - where a programmer makes the computer perform tasks as the resources become available as opposed to executing them in the order received; (8) *Scavenging* - searching for residual data left in a computer

relation to two of the more popular classifications.

Everyone is familiar enough with world history to remember the tale of the "Trojan Horse," in which the Greeks constructed a vehicle and entered the well-protected city. Once inside, the vehicle opened and unleashed an army which furiously attacked, and ultimately subdued, the surprised inhabitants. Computer abusers have a similar vehicle—a program routine secretly hidden inside another program which, once inside the computer's protected environment, escapes and disrupts the computer's operations.[86]

Trojan Horse programs have also been identified as trapdoors, logic bombs, or time bombs.[87] Closely related to the Trojan Horse is the computer "virus." Although there is some dispute over the proper definition of a virus, it is clear that a virus has the capacity to erase other programs or replicate itself onto different programs and computer systems.[88] This is a relatively new phenomenon, and is closely related to the more established classification of "superzapping," which involves the unauthorized use of a computer program to alter, destroy, or copy stored data.[89]

Computer viruses, like viruses that afflict humans, spread through unsuspecting computer systems very quickly. Infections to other computer systems usually occur when an unsuspecting user runs a virus-infected program through a computer network. Also like the human disease, the virus may be either benign or malignant.[90] However, the major concerns lie with the ill-willed virus which can cripple a computer network.

The most infamous example of the damage a virus can cause occurred on November 3, 1988, and was dubbed "the largest virus outbreak thus far in the nation."[91] A computer science graduate student

---

after a job execution; (9) *Data Leakage* - involves the wide range of crimes resulting from the removal of data or copies from a system; (10) *Piggybacking & Impersonation* - involves sending unauthorized signals, or gaining similar access by following closely or on top of a legitimate signal or by simply typing in another authorization code; (11) *Wiretapping* - important due to the connectivity of systems and networks but not used much because of the many easier ways to modify data; and (12) *Simulation & Modeling* - taking an existing process and implementing it elsewhere for improper means. I. SLOAN, *supra* note 4, at 9-18.

86. R. PERRY, *supra* note 56, at 60.

87. I. SLOAN, *supra* note 4.

88. L.A. Daily J., Nov. 15, 1988 at B1, col. 1.

89. I. SLOAN, *supra* note 4.

90. The first computer viruses date back to the early 1970's in university computers. Chicago Daily L. Bull., May 2, 1988, at 8, col. 1. *See also* F. HUBAND & R. SHELTON, *supra* note 2, at 247 (discussing the marketing of software (Vault Corporation and Defendisk) which makes unauthorized copying cause an error in the user's operating system); Note, *supra* note 3, at 628.

91. Note, *supra* note 3, at 625.

allegedly intended to spread a "harmless" virus program through Arapnet, a Department of Defense computer network.[92] The one-day epidemic spread throughout the country wherever local system links were located, and filled the network with extraneous computer information, which, in many instances, overloaded the system and caused a shut down.[93] No data were lost, but authorized users were prevented for an indeterminable time from using the network. In addition, an immeasurable amount of time and money was necessary to purge the network of the unwanted data.[94]

The perpetrator remains under investigation by a federal grand jury and the Justice Department.[95] The investigative panel rejected the idea that the virus was created to point out the need for greater computer security.[96] The havoc created by the virus touched off an interesting debate regarding computer ethics. Indeed, an official at the school where the virus was created stated that "ethics," not increased security, was the best defense against these types of activities.[97] The vice-president of technologies said that he felt it unlikely any security steps could guarantee an impenetrable system.[98] The university felt that these types of activities could be eliminated only through stressing the resultant disharmony caused by such a blatant breach of trust.[99]

While the Arapnet incident attracted some well deserved attention, the fact is that many lesser incidents have occurred in the past, making "computer virus" a household term.[100] Is an emphasis on ethics really what we need, or could we use existing laws to prosecute such an offender in the hopes of deterring respective wrongdoers? As of yet, no prosecution has taken place in the Arapnet case. However, a recent case demonstrates that the government believes that prosecution may be the answer. Federal prosecutors in Chicago obtained the conviction of a teenager who broke into U.S. military computers, in violation of the CFAA.[101]

In a six count complaint, the defendant was charged with violation

---

92. *Id.*

93. *Id.* Many computers have "modems," a term which comes from the words "modulate-demodulate" and are devices which permit computers to be accessed from remote locations through communication circuits.

94. *Id.* at 626.

95. Chicago Daily L. Bull., Apr. 5, 1989, at 5, col. 1.

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. *See* Chicago Daily L. Bull., May 2, 1988, at 8, col. 1. This article also notes some of the ways benign viruses are used, such as season's greetings or advertising notices.

101. United States v. Zinn, No. 88-CW-0673 (N.D. Ill. 1988).

of 18 U.S.C. § 1030(a)(4) to (6).[102] The case record was originally sealed, as the gravity of the offense and types of computers involved made the prosecution believe that doing so would be consistent with governmental security guidelines.[103] However, on the government's motion, this seal was lifted on the theory that such action would further the ends of justice. The U.S. Attorney's Office felt that the court's findings would help the computer community and the public at large realize that the courts would not tolerate unauthorized attacks on computers.[104]

The U.S. Attorney also cited white-collar crime studies and media dramatizations, such as "War Games," as societal barometers, whose messages regarding the acceptability of these actions needed reversal.[105] The government felt that making the case a matter of public record would be helpful in starting such a trend.

The defendant in this case, Herbert Zinn, actually used a Trojan Horse, rather than a virus, in perpetrating his crime.[106] Initially, he unlawfully entered computers owned and operated by AT&T, MIT and the United States Government. Once he entered, he copied proprietary software and destroyed AT&T files.[107] The value of the stolen programs was deemed to be in excess of $1 million.

Zinn was found guilty on five of the six counts in the complaint.[108] Due to his juvenile status, he was sentenced to incarceration at a youth correctional facility for a period of nine months and probation, to commence upon discharge, which would remain in effect until the age of twenty-one. He was also required to make restitution in the amount of

---

102. *Id. See also supra* note 42 and accompanying text.

103. *See Zinn*, N0. 88-CW-0673.

104. *Id.* See Government's Motion to Amend caption of this case and unseal the record.

105. *Id.*

106. Zinn, a native of Chicago, was a seventeen-year old hacker at the time of the offense. He was an only child and a high school dropout with eight arrests; seven as a minor and one as an adult. Most of the arrests were for burglary-type offenses and they generally reflected Zinn's computer involvement. For instance, Zinn stole electronic components from a radio lab and tampered with electronic locks. Zinn had also broken into the computers of the Keller Graduate School of Management in Chicago and the Commodity Prospective Company. Zinn admitted breaking into AT&T computers for a period of more than a year. He further stated that codes were routinely posted on an electronic bulletin board.

107. United States v. Zinn, No. 88 CW-0673 (N.D. Ill. 1988) (Certificate of Jurisdiction and Severity of the Offense).

108. *Id.* at Judgment in a Criminal Case. Zinn was acquitted of a charge under 18 U.S.C. § 1030 (a)(5) and (c)(3)(A) of intentionally accessing a Federal interest computer without authorization and by means of one or more instances of such conduct altering, damaging or destroying information in the Federal interest computer and thereby causing a loss to one or more of a value aggregating $1,000 or more during the month of August, 1987.

$10,000 over a two and one-half year period.[109] The prosecution was limited in its ability to prosecute Zinn to the fullest extent of the law, because of his age. If Zinn had been an adult, he could have faced up to twenty years in a federal correctional facility.[110] However, it is doubtful whether the government would have pushed for such a maximum penalty or that a judge would have given such a harsh sentence. It is important that restitution was ordered in this matter, though one must note that in a case where severe damage is done, the defendant will seldom be able to afford repayments that begin to approach the damage valuation.

Viewing this case in light of the other two prongs of the federal computer crime laws, one could envision more severe penalties. These penalties, of course, would not stem from the Computer Security Act of 1987, for we have seen that it makes no provision for criminal penalties.[111] The quasi-civil remedies available would not be appropriate in this matter.[112] Making a presumption most favorable to the government, we might believe that with the security measures and guidelines called for by the Computer Security Act of 1987 such an incident may be less likely to occur.[113]

Two different provisions of the ECPA may be applicable to the case. The EPCA clearly protects the communications intercepted by the defendant.[114] Zinn's actions of advertising the codes on various bulletin boards were also in violation of the EPCA as advertising a device known to be used for intercepting electronic communications.[115] The remedies available in this case would be both criminal and civil. As the EPCA provides for the greater of $10,000 or $100 a day, Zinn at least would have been liable for $36,500, because he admitted breaking into

109. *Id.*

110. *See supra* note 49 and accompanying text.

111. *See supra* notes 65-68 and accompanying text.

112. At the time of this paper's completion, another Illinois-based computer crime case was being scheduled for trial. In *United States v. Riggs*, 743 F. Supp. 556 (N.D. Ill. 1990), the court made a first impression ruling that the transfer of confidential information from one computer to another constituted a violation of federal law prohibiting the interstate transfer of stolen property. In arguing the applicable laws, both parties cited 18 U.S.C. §§ 1343 and 2314, dealing with interstate transfers and wire fraud. The original indictment charged one of the defendants with violations of the CFAA. However, these charges were later dropped and additional wire fraud charges added. This case appeared to once again highlight the government's fear or misunderstanding of the laws promulgated for the prosecution of such crimes. Chicago Daily L. Bull., June 13, 1990, at 1, col. 1. The case was ultimately dropped by the United States Attorney. Thus Illinois missed its chance to set the interpretational standards for federal prosecution of computer crime under federal statutes designated for the same.

113. *See supra* note 66 and accompanying text.

114. *See supra* note 54.

115. *Id.*

the AT&T computers for more than a year. However, the potential jail time is less than that available under the CFAA.

Interestingly, there is no provision that marks the mutual exclusivity of the CFAA and ECPA. In fact, if computer crime gets as sophisticated as predicted, there may be prosecution under both these laws in the future.

The evidence gathered by the federal enforcement agencies involved in the *Zinn* case was initially provided to the Cook County State's Attorney's office. However, both the Criminal and Juvenile Divisions refused to prosecute the defendant in the circuit courts of the State of Illinois.[116] Again, viewing the decision in the light most favorable to the government, the decision not to prosecute was probably the direct result of the likelihood of conviction under the existing statute.[117] The existing statute proscribed the unlawful use of a computer. The statute defined unlawful use as knowingly accessing, or gaining use of a computer where computer programs are altered or destroyed, or where money, property, or services are obtained from the computer owner.[118] This language easily could have been judicially interpreted to cover Zinn's offenses. The criminal penalties available were not as stringent as those of the federal act actually employed. However, AT&T would have had the opportunity to bring a separate civil suit.[119] Perhaps the State's Attorney was afraid there would be trouble proving Zinn's intent.

The revised Illinois statute became effective on December 1, 1987.[120] The State's Attorney had rejected the *Zinn* case two months earlier. However, applications of the revised statute may have proved more problematic than the one it replaced. Though equipped with a rebuttable presumption in the State's favor, a literal interpretation of the tampering provisions may have fallen short of the intended result. Though Zinn did access the computer and obtain data without authorization, he did not damage or destroy the computer nor did he physically remove data or programs. Thus, he would have been guilty under only the weakest penalty provisions of that section of the Illinois statute and totally would have escaped prosecution for aggravated tampering. For the same reasons, he may have been limited to a minor sanction under the computer fraud section of the Illinois statute.[121] Because there was little federal or State precedent, and an inconsistent, diverse range of

116. United States v. Zinn, No. 88-CW-0673 (N.D. Ill. 1988).

117. ILL. ANN. STAT. ch. 38, para. 16-9 (Smith-Hurd 1979).

118. *Id.*

119. *Id.*

120. *Id.* paras. 16D-1 to 16D-7.

121. *Id.* paras. 16D-3, 16D-4.

opinions in other jurisdictions, the State's Attorney probably would have made the same decision.

If *Zinn* were to arise in 1990, the State would have additional language to consider. A new amendment has been added to the Illinois statute's computer tampering provisions which more specifically addresses the actions of perpetrators like Zinn.[122] The additional section specifies that "computer tampering" also includes the insertion or attempted insertion of a program into a computer with knowledge that this activity may damage or destroy that computer or any other computer.[123] It also prohibits activity which may alter, delete, or remove a program or data, or which may cause a loss to the users of that computer or another computer which is accessed by a damaging program.[124] The new section also brings back the favored civil remedy provisions, which include attorney's fees and costs.[125]

When the above is read in conjunction with other provisions of the computer tampering statute, it appears that all bases are covered. Access both via an authorized code and by virtue of a program, if done without the authorization of the computer owner, expressly falls within the bounds of the statute. When further viewed in relation to the definition sections, the Illinois statute clearly encompasses the use, alteration, damage or destruction of a computer, computer system, computer network or any computer software in place in such a device.[126] However, problems may still exist in implementing the statute in that it may be difficult to determine which individual inserted the offending program knowing or having reason to believe that damage would result[127]

Another potential area of difficulty in applying the Illinois statute may occur where accessing is done without a program for the purpose of entering a benign virus which, for some reason, ultimately goes haywire. A virus normally carries no source identifier. With the germs replicating themselves throughout a computer network, it becomes dif-

122. P.A. 86-762, § 1 (Senate Bill 1153) (amending ch. 38, paras. 16D-3, approved Sept. 1, 1989, effective Jan. 1, 1990).

123. *Id.* The section reinforces the rebuttable presumption of the statute (para. 16D-7) in that it finds liable one who even has reason to believe that damage will occur. The interpretation may prove to be unnecessarily difficult, however, since the preface to the section explicitly states one must "knowingly" violate one of the subsections.

124. *Id.* para. 16D-3(a)(4).

125. *Id.* para. 16D-3(c).

126. This is the language of prohibition stated in Colorado Revised Statutes section 18-5.5-102 (1986), which some have suggested more thoroughly covers "Zinnish" activities. The remedies available under this statute are also weaker than the Illinois statute.

127. In the rest of the section relative to accessing, one might assume that it would be easier to trace back to the point of unauthorized access as this involves different methods than those associated with Trojan Horses and viruses.

ficult to know who to prosecute. Many times these viruses are programmed to read a computer's system clock and may not flare into a debilitating illness until months or years later.[128] In situations like this, increased ethics and awareness seem to be the only recourse. Like any disease, preventive medicine is usually the best cure.[129]

Another point of reference for the ethics vote is a lack of consistent prosecutions for computer crimes. Even the prosecution in *Zinn* noted this problem. They cited as possible reasons both the fear of embarrassment and bad publicity from such a disclosure.[130] Others claim that the weak remedial sections are not cost effective compared to the amount of involvement necessary in working with numerous federal enforcement agencies.[131] Still others are afraid to call attention to the lack of security within their system or are afraid that the perpetrator will be a "Zinnish" youth who is not worth prosecuting at all.

In addition, the authorities are ambivalent about prosecuting. The reasons for this appear to be a lack of understanding of the technology involved in the crime, the tediousness of preparing a case, the attitude that the perpetrators are clever and misguided as opposed to the typical criminal makeup, and the fact that most of the aggrieved parties are banks or big businesses as opposed to individuals.[132] Again, the prosecution looks at the lack of "byte" in the penalty provisions as hardly being worth the time to pursue a case. With such views, the deterrence effect of computer crime statutes is almost entirely nonexistent on both the federal and state levels. Certainly, with more prosecutions, the desired effect may be reached. States like Illinois have added to this possibility by making provisions for civil actions.

Whether the preoccupation with viruses is even warranted is debatable. Despite all the reasons set forth above, some still argue that vi-

---

128. Kenyon, *The Computer Contagion*, 75 A.B.A. J. 116 (1989).

129. *Id.* at 117, suggesting ten helpful tips for avoiding viruses:

1) Do not copy strange software onto your hard disk without testing it.

2) Be wary of commonly circulated software from electronic bulletin boards and friends.

3) Take note of the file size and creation date of frequently used operating files.

4) Consider storing executable files in hidden subdirectories.

5) Use the ATTRIB.COM command to change the file attribute for executable files to read only.

6) Do not let just anybody use your computer.

7) Establish a clear, concise office policy regarding computer usage.

8) Obtain fresh copies of widely circulated software.

9) Keep a proper backup of important material.

10) Do not panic.

130. *See supra* note 99.

131. *Id.*

132. *See* Note, *supra* note 3, at 630.

ruses are just not that common, and as such, deserve a correspondingly low degree of attention.[133]

VI. SIGNING OFF

Contrary to the norm in cases involving computer crimes, the lessons of history are few. As to viruses and their kindred, tactics for prevention are certainly best. Many of the suggestions in this area are common sense; however, the market has also seen an ever burgeoning product line of so called vaccines set to immunize ailing systems in the community.[134]

As for computer crimes in general, a federal guideline could still prove useful. Although three major acts set forth regulations on computer misdoings, neither is the language specific enough, nor the jurisdictional provisions broad enough, to provide for comfortable judicial implementation. Possibly with more findings such as that in the *Zinn* case, a body of law can develop which can set forth some guidance.

The states have taken great steps toward enacting responsive legislation themselves; however, they too have been reluctant to make wholesale findings in a manner that can provide consistency to a reader seeking knowledge or guidance to a judiciary straining for proper interpretation. By providing for civil and criminal remedies, states like Illinois are at least enhancing the possibility that such a body of law may become established.

The computer community would probably best be served by the federal government's adoption of a uniform computer crime statute. The states would then be given the opportunity to establish little interpretive legislation, which would only need to be at least as restrictive as the model legislation. Similar approaches have worked well with other bodies of law such as the Federal Trade Commission Act and the Uniform Commercial Code. Until such time as these types of steps are taken, we will continue to be faced with widely divergent state decisions, limited federal directives, and the old world hope for the power of ethical considerations in an increasingly technological society.

133. *See supra* note 90.

134. *See supra* note 128, at 117. *See also* F. HUBAND & R. SHELTON, *supra* note 2 (discussing products such as "Bomb Squad" and "Flu Shot" and a list entitled the "Dirty Dozen" which keeps electronic bulletin boards aware of troublesome "Shareware"). *See also* R. PERRY, *supra* note 56 (predicting futuristic securing measures to include voice recognition, finger scanners and eyeball scanners which compare retina patters to determine if access is allowable).