Vanderbilt Law Review

Volume 43
Issue 2 *Issue 2 - March 1990*

Article 4

3-1990

The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem

Dodd S. Griffith

Follow this and additional works at: https://scholarship.law.vanderbilt.edu/vlr

 Part of the Computer Law Commons, and the Internet Law Commons

Recommended Citation
Dodd S. Griffith, The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem, 43 *Vanderbilt Law Review* 453 (1990)
Available at: https://scholarship.law.vanderbilt.edu/vlr/vol43/iss2/4

This Note is brought to you for free and open access by Scholarship@Vanderbilt Law. It has been accepted for inclusion in Vanderbilt Law Review by an authorized editor of Scholarship@Vanderbilt Law. For more information, please contact mark.j.williams@vanderbilt.edu.

NOTES

The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem

Only a hermit would be unaware of the degree to which computers have permeated every aspect of our lives. From the cradle to the grave our activities are influenced, tracked, recorded and controlled by computers. Virtually every public and private employee comes in contact with a computer in some capacity during the work day. The possibilities of computer fraud are mindboggling. Those who deal with these machines and develop the required expertise must be deterred from

using their skills to the detriment of their employers and others.[1]

I. INTRODUCTION

Before the invention of the computer, the amount of property an individual could steal or destroy was, to some extent, determined by physical limitations.[2] Criminals could take only as much property as they could carry or arrange to transport.[3] For example, the average amount of money taken in a bank robbery has been estimated to be about ten thousand dollars.[4] Crime has, however, changed with the times.[5] A criminal can use modern technology to transfer extremely large sums of money that formerly would have been impossible to remove without detection.[6] A 1984 study conducted by the American Bar Association Task Force on Computer Crime (the ABA Task Force Report) estimates computer crime losses to be approximately 100,000 to 500,000 dollars per instance.[7] Although the disparity between the dollar figure reported in the ABA Task Force Report and the estimate of the average amount seized in a manual bank robbery might seem alarming in its own right, these figures barely hint at the most alarming aspect of the computer crime phenomenon: its potential for growth.

American businesses, universities, and research organizations currently use an estimated 56,000 large general purpose computers and 213,000 smaller business computers.[8] The private business sector uses an additional 570,000 mini-computers and 2.4 million desktop computers.[9] Moreover, in 1982 the Federal Government owned more than

---

1. Tennessee v. Edmondson, No. 87-176-III (Tenn. Crim. App. Mar. 1988), *reprinted in part in* 7 COMPUTER L. REP. 375, 376 (1988).

2. *See* Nawrocki, *Special Report: There are too Many Loopholes; Current Computer Crime Laws Require Clearer Definition*, DATA MGMT., July 1987, at 14.

3. *See id.*

4. *See id.*

5. *See id.*

6. *See id.*

7. *See* A.B.A., CRIMINAL JUSTICE SECTION, TASK FORCE ON COMPUTER CRIME, REPORT ON COMPUTER CRIME (1984). The ABA Task Force surveyed over 1000 corporations, banks, professional service firms, and state and federal agencies concerning their experiences with and awareness of computer crime. Two hundred and thirty-eight firms and agencies responded. *Id.* at 16. More than one-quarter of the respondents stated that they had experienced known and verified losses from computer crime during the prior 12 months. *Id.* at 38. The responses indicated that annual loss from computer crime was between $145 and $730 million, depending on whether the respondent's estimated losses fell within the high or low end of the range of the amounts they had reported. *Id.* These figures indicate that the average loss per respondent was between $2 and $10 million per year. *Id.* The ABA Task Force concluded that management and the public may be underestimating the size of the problem.

8. 132 CONG. REC. H3277 (daily ed. June 3, 1986) (statement of Rep. William Nelson) [hereinafter Nelson Statement].

9. *Id.*

15,000 computers.[10] Studies indicate that the trend to computerize will continue at a rapid pace.[11] The number of computers outside the realm of business and government is growing rapidly as well. An estimated six million home computers were in use in 1986.[12] That figure is expected to grow exponentially in the next few years.[13] In addition, home computers are expected to be connected with the data banks of major institutions such as banks and retail stores.[14] These figures illustrate the burgeoning potential for computer abuse by members of the general populace. The computer is no longer solely the tool of a few highly trained technocrats. It has been delivered to a public that has embraced its potential eagerly.[15] Because computers may be used for destructive as well as constructive purposes, their proliferation has forced Congress, in considering the need for and effectiveness of federal computer crime legislation, to search for legislative solutions that will prove suitable to the society of computer users that it foresees in the immediate future.[16]

On October 12, 1984 legislators passed the first federal statute prohibiting specific acts involving the use of a computer.[17] This legislation, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (the 1984 Act), prohibited computer related activity in only a few relatively narrow areas.[18] The decision to pass a statute that limited federal intervention to certain specific situations reflected legislators' realization that the scope of the computer crime problem was not

---

10. *Id.* In addition, "[t]he General Services Administration estimates that there will he 250,000 to 500,000 computers in use by the Federal Government by 1990." S. REP. No. 432, 99th Cong., 2d Sess. 2, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 2479, 2479.

11. *See* FINAL REPORT: SMALL BUSINESS COMPUTER SECURITY EDUCATION AND ADVISORY COUNCIL, *published in* 7 COMPUTER L. REP. 525 (1988). Thirty to thirty-five percent of the seventeen million small businesses (under five hundred employees) in existence in 1985 used computers. *Id.* at 530. That figure rose to more than 65% hy 1987. Moreover, the report stated that "the computer is used in a far more pervasive manner than just automating the word processing and accounting operations." *Id.*

12. Nelson Statement, *supra* note 8, at H3278.

13. *Id.*; *see also* H.R. REP. No. 612, 99th Cong., 2d Sess. 3 (1986) (stating that an estimated 90 million home computers will be in use by 1999). "The exponential increase in the use of computers also can be seen in the sale of software for personal computers. In 1976 these sales were essentially zero hut hy the end of 1982 they were $1 billion." *Id.* at 5; S. REP. No. 432, *supra* note 10, at 2, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS at 2479 (stating that "[i]n 1978, there were an estimated 5,000 desk-top computers in this country; today there are nearly 5 million").

14. Nelson Statement, *supra* note 8, at H3278.

15. *See id.* at 3277; *see also* Bloombecker, *New Federal Law Bolsters Computer Security Efforts*, COMPUTERWORLD, Oct. 27, 1986, at 53 (discussing the "democratization" of computer crime).

16. *See* S. REP. No. 432, *supra* note 10, at 2-3, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS at 2479-81.

17. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (1984) (codified as amended at 18 U.S.C. § 1030 (1988)) [hereinafter 1984 Act].

18. *See id.; see also infra* Part II(A).

well known and that their actions might have unforeseen repercussions.[19] Legislators considered and rejected broader bills that criminalized the use of a computer as a part of a scheme to defraud that affected interstate commerce,[20] choosing instead to protect only the most vital federal interests that could be injured by computer users.[21]

The 1984 Act, however, was criticized for numerous substantive and structural defects.[22] Congressional sponsors of computer crime legislation responded to this criticism by introducing several additional bills for committee review.[23] These bills and the ensuing committee hearings addressed the criticisms of the 1984 Act.[24] The Computer Fraud and Abuse Act of 1986[25] (the 1986 Act) was the final product of this refinement process.

The primary goal of this Note is to discuss the changes brought about by the adoption of the 1986 Act and the policy reasons that form the basis for those changes.[26] A secondary goal is to explain why Congress has exercised moderation in this area of legislation and to discuss how existing legislation may be improved. Part II of this Note summarizes the provisions of the 1984 Act, analyzes their function and structure, and discusses the criticisms offered by various commentators. Part III summarizes the changes embodied in the 1986 Act, discusses the

---

19. *See* Betts, *Private-Sector Computer Crime Bill Faces Fire at Hearing*, COMPUTERWORLD, June 3, 1985, at 15 (noting that "[r]epresentatives of the American Civil Liberties Union and the American Society of Newspaper Editors expressed concern that the Computer Fraud and Abuse Act of 1984 may inhibit government whistle-blowers from disclosing computer-stored information about fraud and abuse in federal programs").

20. *See, e.g.*, H.R. 3570, 98th Cong., 1st Sess. (1983).

21. *See* S. REP. No. 432, *supra* note 10, at 4, *reprinted in* U.S. CODE CONG. & ADMIN. NEWS at 2482.

22. *See* Tompkins & Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem*, 6 COMPUTER L. J. 459, 471-81 (1986). Federal prosecutors, for instance, complained that the 1984 Act was not an effective tool for prosecution. *See Computer Fraud Legislation: Hearing Before the Subcomm. on Criminal Law of the Senate Comm. on the Judiciary*, 99th Cong., 1st Sess. 25 (1985) (statement of Victoria Toensing, Deputy Assistant Attorney General, Criminal Division, Department of Justice) [hereinafter *Computer Fraud Hearing*]. Federal prosecutors apparently used the statute on only a few isolated occasions and testified that prosecution under other statutes would be preferable in many instances. *See* Tompkins & Ansell, *Computer Crime: Keeping Up With High Tech Criminals*, CRIM. JUST., Winter 1987, at 31. "To our knowledge, only one person has been indicted under the 1984 law. (*United States v. Fadriquela*, No. 85-CR-40, U.S. Dist. Ct. (D. Colo. 1985); in May 1985 Mr. Fadriquela pleaded guilty to misdemeanor charges under the Act and was fined $3000)." *Id.* at 32; *see Computer Fraud Hearing*, *supra* (describing why an existing espionage statute would be preferable to prosecute an act that theoretically could be prosecuted under the 1984 Act).

23. *See* Tompkins & Mar, *supra* note 22; *see also The Computer Fraud and Abuse Act of 1986: Hearing on S.2281 Before the Senate Comm. on the Judiciary*, 99th Cong., 2d Sess. (1986).

24. *See supra* note 23.

25. Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (1988)) [hereinafter 1986 Act].

26. *See infra* Parts II & III.

policy judgments they reflect, and attempts to surmise whether these changes accomplished their respective goals with particular emphasis on the need to increase the deterrent value of the Act. Part IV discusses an alternative policy toward deterrence that Congress did not incorporate in the 1986 Act and that may have undercut the deterrent impact of other changes. Finally, Part V argues that to enhance the deterrent value of the Act, Congress should require victims of computer crime to take precautions to protect themselves and to report violations in addition to its current strategy of facilitating prosecution and increasing sanctions.

The extensive body of legislative history and industry articles that have appeared over the last few years provide a relatively clear picture of why Congress chose to amend the 1984 Act as it did.[27] This Note uses that body of material to examine the manner in which the 1984 Act was intended to function, the criticisms of its actual function, and the congressional rationale for its passage. An examination of the evolution of the law provides the contrast needed to grasp the significance of the changes and helps elucidate the policy considerations that surround the area of computer crime legislation.

II. THE COUNTERFEIT ACCESS DEVICE AND COMPUTER FRAUD AND ABUSE ACT OF 1984: THE FIRST ATTEMPT AT FEDERAL COMPUTER CRIME LEGISLATION

A. *Scope and Structure of the 1984 Act*

1. Background of the 1984 Act

Representative William Nelson, when confronted with the dilemma of trying to devise effective and acceptable federal computer crime legislation, hypothesized that the growing popularity of computers among the general populace would create conflicts analogous to those that legislators have encountered when they have attempted to pass gun control legislation.[28] He commented that computer crimes are not crimes

---

27. *See* 132 CONG. REC. S14,456 (daily ed. Oct. 1, 1986) (statement of Sen. Paul Laxalt). Senator Laxalt noted:

> [The Senate had attempted] to establish the most complete legislative history possible to provide information about the intended meaning of the legislative language. . . . Because of the complexity of the subject matter, we wanted to be as certain as we could that the limits and the intended scope of this bill be clear to prosecutors and computer users alike.

Id.

28. Nelson Statement, *supra* note 8, at H3277. Representative Nelson stated:

> Computers may not commit crimes—any more than guns commit crimes. But we have to be realistic—there are people who will commit crimes with guns if they are readily available, and there are people who will commit crimes with computers as they become ubiquitous in

committed by computers, but are crimes committed by people assisted by computers.[29] The Congressman thus concluded that banning computers would be as impractical as banning ownership of guns.[30] He observed that both items are potentially dangerous, but both are considered essential forms of private property by many members of our society. Consequently, the question for legislators studying the need for a federal computer crime statute became how much control was appropriate.[31]

Congress originally seemed to believe that specific computer crime legislation was not necessary.[32] This initial restraint can be attributed to two concerns: redundancy[33] and fear of federal overreaching.[34] Witnesses at committee hearings on the need for a federal computer crime statute testified that forty to fifty existing federal statutes could be used to prosecute computer assisted crimes.[35] As a result, committee members questioned the need for an additional federal statute.[36] Legis-

---

> our society. I doubt, frankly, that we can address the problem of crime by banning either. Americans may not now be as attached to their computers as they are to their guns, but I suspect they will be inseparable before too long.

Id.

29. *Id.*

30. *Id.*

31. *See* S. REP. No. 432, *supra* note 10, at 4, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS at 2482.

32. *See* Tompkins & Mar, *supra* note 22. Despite the introduction of more than a dozen computer crime bills since 1979, Congress adopted no specific computer crime legislation until 1984. *Id.* at 460 n.2; *see also* Hollinger & Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 110 (1988) (stating that "[d]espite the impressive array of testimony supporting a federal statute, no House or Senate committee could be convinced that the federal government should play a specific role in controlling computer crime").

33. *Computer Crime: Hearing Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 98th Cong., 1st Sess. 5, 6 (1983) (statement of Rep. George Gekas) [hereinafter *Computer Crime Hearing*]; *see also Computer Security in the Federal Government and the Private Sector: Hearings Before the Subcomm. on Oversight of Government Management of the Senate Comm. on Governmental Affairs*, 98th Cong., 1st Sess. 40-41 (1983) (statement of Sen. William Cohen) [hereinafter *Computer Security Hearings*]; *id.* at 72-73 (statement of Richard P. Kusserow, Inspector General, Department of Health & Human Services); *id.* at 138-39 (statement of John C. Keeney, Deputy Assistant Attorney General, Criminal Division, Department of Justice); Hollinger & Lanza-Kaduce, *supra* note 32, at 110.

34. *See Computer Crime Hearing*, *supra* note 33, at 29, 30 (statement of Rep. Robert Kastenmeier); *see also Unauthorized Access to Individual Medical Records: Hearing Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 98th Cong., 2d Sess. 6-7, 10 (1984) (statement of John C. Keeney, Deputy Assistant Attorney General, Criminal Division, Department of Justice); *id.* at 16-17 (statement of Rep. Ron Wyden).

35. *See Computer Security Hearings*, *supra* note 33, at 9 (statement of Susan H. Nycum, Partner, Gaston, Snow & Ely Bartlett, Palo Alto, Ca.); *id.* at 40 (statement of August Bequai, Counsel to the American Society for Industrial Security); *see also* Thackeray, *Computer-Related Crimes, An Outline*, 25 JURIMETRICS J. 300 (1985) (outlining many of the federal statutes applicable to computer crime in 1984).

36. *See supra* notes 33-35.

lators also were concerned that a federal computer crime statute might have an adverse effect on state prosecution of computer crimes.[37] Approximately twenty-one states had enacted computer crime legislation by 1983.[38] This proliferation of state computer crime statutes and the imminent prospect of enactment of computer crime legislation in the remaining states caused members of the House Judiciary Committee to question the propriety of federal legislation covering the same issues.[39] An additional concern was the breadth of any statute recommended by the committee. A broad preemptive statute would ensure uniformity among states. A narrower statute, alternatively, would limit federal jurisdiction to specific situations.[40]

The lack of accurate information also hindered the committee process.[41] The only information available was anecdotal[42] or based on inconclusive[43] or unscientific[44] polls. In addition, at least one witness questioned, in the absence of any hard data, the existence of any significant computer crime problem as of the time of his 1983 testimony[45] and doubted the propriety of federal legislation in the absence of a clearer

---

37. *See Computer Crime Hearing, supra* note 33, at 27-31 (reporting discussion between John C. Keeney, Deputy Assistant Attorney General, Criminal Division, Department of Justice and various committee members).

38. *See id.* at 2 (statement of Rep. William Nelson).

39. *See id.* at 5 (statement of Rep. George Gekas); *id.* at 29 (statement of Rep. Robert Kastenmeier).

40. *Id.* at 29 (statement of Rep. Robert Kastenmeier).

41. *See Federal Computer Systems Protection Act: Hearing Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary,* 97th Cong., 2d Sess. 2-3 (1982) (statement of Roger M. Olsen, Deputy Assistant Attorney General, Criminal Division, Department of Justice) [hereinafter *Federal Computer Systems Protection Hearing*] (citing a 1982 report, "Electronic Fund Transfer Systems and Crime," by the Justice Department's Bureau of Justice Statistics, which found that "no valid data for measuring and understanding the nature and extent of EFT crime" existed); *see also* Hollinger & Lanza-Kaduce, *supra* note 32, at 105-06 (detailing criticism of self-proclaimed experts' estimates of the magnitude of the computer crime problem).

42. *See* Hollinger & Lanza-Kaduce, *supra* note 32, at 105; *supra* note 41; *see also Federal Computer Systems Protection Hearing, supra* note 41, at 38-39 (statement of Milton R. Wessel, General Counsel to the Association of Data Processing Service Organizations). Mr. Wessel has served as an Adjunct Professor of Computer Law at various schools including Stanford University, Georgetown University, and Columbia University.

43. *See Computer Security Hearings, supra* note 33, at 212. The Department of Health and Human Services published a 1983 report, "Computer-Related Fraud and Abuse in Government Agencies," which concluded that "[a]lthough originally charged to discover the scope of computer-related fraud and abuse in Government programs, the task force rapidly became aware that this was not possible."

44. *See Computer Security Hearings, supra* note 33, at 170-72. The hearing report includes the 30 question survey and accompanying cover letter that the American Society for Industrial Security sent to its members as part of its effort to prepare evidence to present to the Senate Subcommittee on Governmental Affairs. The survey generated 637 responses for a 29% return rate. *Id.* at 163.

45. *See Federal Computer Systems Protection Hearings, supra* note 41, at 17, 39 (statement of Milton R. Wessel).

understanding of the nature of the problem.[46] That testimony echoed the concern of some congressmen present at the committee hearing.[47]

A sequence of events in 1983 and 1984, however, overshadowed the concerns that had caused Congress to delay passage of a federal computer crime statute.[48] The American Bar Association and other public and private associations first directed attention to the issue by publishing several studies on computer crime.[49] The impact of these reports later was magnified by a groundswell of media attention toward computer crime generated by a number of incidents involving juvenile computer hackers.[50] These news reports created an impression that computer crime was a major problem for which an immediate solution was needed.[51] Responding to these new stimuli, Congress soon passed the 1984 Act.

2. Summary of the 1984 Act

The 1984 Act prohibited the unauthorized use of or access to a computer in three comparatively narrow areas. First, the Act made it a felony knowingly to access a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information with the intent or reason to believe that such information would be used to harm the United States or to advantage a foreign nation.[52] Second, the 1984 Act made it a misdemeanor knowingly to access a computer without authorization, or in excess of authorization, in order to obtain information contained in a financial record of a financial institution or in a consumer file of a consumer reporting agency.[53] Third, the 1984 Act made it a misdemeanor knowingly to access a computer without authorization, or in excess of authorization, in order to use, modify, destroy, or disclose information in, or prevent authorized use of, a computer operated for or on behalf of the United States if such conduct would affect the government's use of the

---

46. *Id.* at 17.

47. *See Computer Crime Hearings*, *supra* note 33, at 7-8 (statement of Rep. Dan Glickman); *id.* at 29 (statement of Rep. Robert Kastenmeier) (discussing the possibility of appointing a national commission to study computer issues).

48. *See* Tompkins & Mar, *supra* note 22, at 460; *see also* Hollinger & Lanza-Kaduce, *supra* note 32, at 106-07.

49. *See* Tompkins & Mar, *supra* note 22, at 460 n.3; *see also* Hollinger & Lanza-Kaduce, *supra* note 32, at 108 (noting that "[t]he ABA released a survey purporting to show significant business and government victimization from computer crime immediately prior to the vote in 1984 on the first federal law").

50. *See* Hollinger & Lanza-Kaduce, *supra* note 32, at 106-07.

51. *Id.* at 107.

52. 1984 Act, *supra* note 17, § 1030(a)(1) (current version at 18 U.S.C. § 1030(a)(1) (1988)).

53. *Id.* § 1030(a)(2) (current version at 18 U.S.C. § 1030(a)(2) (1988)).

computer.[54] The 1984 Act also made it a crime to attempt or to conspire to commit any of the three acts described above.[55]

The Act provided enhanced penalties for repeat offenders[56] and empowered the Secret Service, along with other agencies, to investigate offenses.[57] The 1984 Act further specified that the Attorney General and the Secretary of the Treasury were to enter into an agreement defining the scope of the Secret Service's investigative authority.[58]

3. Analysis of the Provisions of the 1984 Act

The 1984 Act made knowing and unauthorized access to or use of a computer beyond the scope of legitimate access the threshold requirements for prosecution.[59] The parameters of these requirements depended on the meaning of the terms "without authorization," "beyond authorization,"[60] "access," "computer," and "use," because no prosecution was possible unless a person "accessed" or "used" a "computer" without or beyond "authorization." The 1984 Act, however, defined only one of these terms, "computer."[61] The adopted definition of "computer" was intended to limit the type of activity prohibited under the 1984 Act by explicitly excluding automated typewriters, typesetters, hand held calculators, and other similar devices.[62] This exclusion helped to ensure that the legislation did not prohibit conduct which Congress did not intend to proscribe.[63] Once the threshold requirements were met, the 1984 Act created criminal liability only for the un-

---

54. *Id.* § 1030(a)(3) (current version at 18 U.S.C. § 1030(a)(3) (1988)).

55. *Id.* § 1030(b)(2) (current version at 18 U.S.C. § 1030(b)(2) (1988)).

56. *Id.* § 1030(c) (current version at 18 U.S.C. § 1030(c) (1988)).

57. *Id.* § 1030(c) (current version at 18 U.S.C. § 1030(d) (1988)).

58. *Id.*

59. *Id.* § 1030(a)(1) (current version at 18 U.S.C. § 1030(a)(1)(1988)). Each of the subparagraphs of 18 U.S.C. § 1030(a) specified that the 1984 Act applied only to persons who "knowingly acces[sed] a computer without authorization, or having accessed a computer with authorization, us[ed] the opportunity such access provide[d] for purposes to which such authorization d[id] not extend." *See, e.g., id.*

60. *See, e.g., id.* (limiting violations to accesses "for purposes to which . . . authorization does not extend").

61. *Id.* § 1030(e) (current version at 18 U.S.C. § 1030(e)(1988)). 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.

62. *Id.*

63. *See* Tompkins & Mar, *supra* note 22, at 463 n.17. In contrast, most of the states that had computer crime statutes at the time of the enactment of the 1984 Act provided broad statutory definitions of "computer" that did not exclude such items. *Id.* at 463. The statutes thus could be construed to cover acts that the states probably had no intention of prohibiting.

authorized activities described in the three subsections of section 1030(a).[64]

Subsection (a)(1) prohibited the use of a computer to obtain classified defense, foreign relations, and nuclear information.[65] Congress narrowly circumscribed the types of information to be protected under this subsection by reference to existing legislation.[66] The House Judiciary Committee modified the language in the proposed subsection so that the list of protected information would conform to the definition of classified information spelled out in the Classified Information Procedures Act.[67] In addition, the Committee added "bad faith" as a prerequisite to prosecution so that the 1984 Act would not extend liability beyond existing espionage laws.[68] These changes appear to have served the dual congressional goals of limiting the scope of the proposed legislation to reduce the chances of unintended effects and of providing useful language for prosecuting offenders.

Subsection (a)(2) prohibited the use of a computer to access without authorization information contained in a financial record of a financial institution or contained in a consumer file of a consumer reporting agency.[69] The subsection protected the types of information encompassed by the Right to Financial Privacy Act of 1978[70] and the Fair Credit Reporting Act.[71] Subsection (a)(2) used the terms "financial institution," "financial record," "consumer reporting agency," and "consumer" as they were defined in those Acts.[72]

---

64. *See* 1984 Act, *supra* note 17, § (a) (current version at 18 U.S.C. § 1030(a) (1988)).

65. *Id.* § 1030(a)(1) (current version at § 1030(a)(1) (1988)).

66. *See* H.R. REP. No. 894, 98th Cong., 2d Sess. 21 (1984).

67. *Id.*

68. *Id.* at 21. The House Judiciary Committee stated that the Committee adopted the language "with intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation" because the Supreme Court in Gorin v. United States, 312 U.S. 19, 28 (1941), interpreted espionage law to require a showing of bad faith before sanctions could be applied. H.R. REP. No. 894, *supra* note 66, at 21 (citing 18 U.S.C. § 793 (1982)).

69. *See* 1984 Act, *supra* note 17, § 1030(a)(2) (current version at 18 U.S.C. § 1030(a)(2) (1988)).

70. 12 U.S.C. §§ 3401-3422 (1988).

71. 15 U.S.C. §§ 1681-1681t (1988).

72. The Right to Financial Privacy Act of 1978 defines a "financial institution" as "any office of a bank, savings bank, [credit] card issuer, . . . industrial loan company, trust company, savings and loan, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in [the United States and its territories]." 12 U.S.C. § 3401(1) (1988). A "financial record" is defined as "an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution." *Id.* § 3401(2).

The Fair Credit Reporting Act defines a "consumer reporting agency:"

> [A]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit infor-

The subsection, by referring to the Right to Financial Privacy Act of 1978, made it a misdemeanor to access without authorization a computer maintained by a "financial institution" and thereby obtain information relating to an individual or a partnership of five or fewer individuals, if such information could be identified with, or be identified as having been derived from, the financial records of a particular customer.[73] The referenced provision did not apply to information that could not be associated with a specific person.[74] The reference to the Fair Credit Reporting Act made it a misdemeanor to access without authorization "consumer reporting agency" files relating to an individual's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.[75] Although subsection (a)(2) defined the types of financial information protected by reference to the Right to Financial Privacy Act of 1978 and the Fair Credit Reporting Act, its prohibitions applied to all persons rather than adopting the more limited protection granted under those Acts.[76]

The House Judiciary Committee emphasized that subsection (a)(2) was not intended to encompass information incidentally obtained or the use of information that was obtained legitimately[77] and attempted to ensure that the provision would not be construed to prohibit computer access for legitimate business purposes.[78] The report made clear that the sole purpose of the subsection was to deter hackers and other criminals from accessing computerized financial files without authorization.[79] Thus, unlike subsection (a)(1), subsection (a)(2) did not require that the information be obtained with intent to injure any person.[80] Un-

---

mation or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f) (1988). A "consumer" is defined as an "individual." *Id.* § 1681a(c).

73. *See* 12 U.S.C. §§ 3401(4), 3402 (1988).

74. *See id.* § 3413(a).

75. *See* 15 U.S.C. §§ 1681-1681t (1988).

76. *See* H.R. REP. No. 894, *supra* note 66, at 21. The Financial Privacy Act of 1978 applies only to federal employees. The House Judiciary Committee Report on the 1984 Act, however, states that being associated with or employed by the government is not a prerequisite to prosecution. *See id.* Presumably, Congress intended the subsection to be read in the same way with regard to the Fair Credit Reporting Act, which applies only to consumer reporting agencies.

77. *See id.*

78. *See id.* The Judiciary report stated that "any access for a legitimate purpose that is pursuant to an express or implied authorization would not be affected. The provision does not extend to normal and customary business procedures and information usage and so these legitimate practices will not be interrupted or otherwise affected." *Id.*

79. *Id.* at 21, 22; *see also id.* at 10, 11 (recounting testimony that influenced the Committee's view on subsection (a)(2)); 130 CONG. REC. H6315 (daily ed. June 22, 1984) (statement of Rep. William Hughes) (indicating that subsection (a)(2) was added because of congressional concern about incidents such as the intrusion into one company's computer credit files in 1984).

80. *Compare* 1984 Act, *supra* note 17, § 1030(a)(1) (current version at 18 U.S.C. § 1030(a)(1)

authorized access alone was enough to trigger liability.[81]

Subsection (a)(3) made it a misdemeanor to use, modify, destroy, or disclose information in, or to prevent authorized use of, a computer operated for or on behalf of the United States if such conduct would affect the government's use of the computer.[82] The final phrase limited the scope of the subsection by requiring the government to prove that the unauthorized access affected a government computer operation.[83] Furthermore, if the government only used a computer on a part-time basis, subsection (a)(3) would apply only if the prohibited conduct substantially affected the government's operation of that computer.[84] The House Judiciary report stated that if such conduct did not substantially affect a government computer operation, the unauthorized conduct would have to qualify as an act prohibited by subsection (a)(2) to be prosecuted under the 1984 Act.[85]

Subsection (a) concluded by setting out a use exemption to subsections (a)(2) and (a)(3).[86] The use exception excluded from subsection (a)(3) actions that otherwise would have been violations if they were committed by a person authorized to access a government computer and that person exceeded such authorization solely by using the computer's capacity for innocuous activities like doing homework or playing computer games.[87] The Judiciary Committee felt that such conduct should be deterred by more informal administrative proceedings.[88]

The Judiciary Committee report did not explain the purpose of a use exemption for subsection (a)(2).[89] The legislation on which the

---

(1988) *with id.* § 1030(a)(2) (current version at 18 U.S.C. § 1030(a)(2) (1988)).

81. *Id.* § 1030(a)(2) (current version at 18 U.S.C. § 1030(a)(2) (1988)); *see also* H.R. REP. No. 894, *supra* note 66, at 22 (stating that "[s]ection 1030(a)(3) is intended to make it a Federal offense to access—with knowledge that the access is unauthorized—this information"). Subsection (a)(3), like subsection (a)(2), did not require that the information be obtained with intent to injure any person.

82. 1984 Act, *supra* note 17, § 1030(a)(3) (current version at 18 U.S.C. § 1030(a)(3) (1988)).

83. *See* H.R. REP. No. 894, *supra* note 66, at 22. The report stated that the "subsection requires that 'such conduct affects such operation'; this phrase is to cover computers which are used only part-time for the U.S. Government. If such conduct does not suhstantially affect the U.S. Government operation, the prosecutions, if any, would have to fall within (a)(3) . . . ." *Id.*

84. *Id.*

85. *Id.*

86. 1984 Act, *supra* note 17, § 1030(a) (current version at 18 U.S.C. § 1030(a) (1988)). The Act stated:

> It is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer.

Id.

87. *See* H.R. REP. No. 894, *supra* note 66, at 22.

88. *Id.*

89. *See id.* at 20-23.

Committee reported did not contain a use exemption for the subsection that became subsection (a)(2) of the 1984 Act.[90] The use exemption in the bill that the Committee considered applied only to subsection (a)(3) of the 1984 Act and a proposed subsection (a)(4), which was deleted before the legislation was enacted.[91] Thus, it seems likely that the use exemption was included accidentally in subsection (a)(2) when the bill was modified hurriedly to get Senate approval in time to be appended to the Comprehensive Crime Control Act.[92]

The use exemption has no logical application to subsection (a)(2). The Judiciary Committee's analysis of subsection (a)(2) expressly emphasized that any unauthorized access which resulted in the computer user obtaining protected information would result in criminal liability under the 1984 Act.[93] The subsection did not require bad faith and excluded from liability only customary business usage that might otherwise have been technically construed as unauthorized access.[94] The application of a use exemption to subsection (a)(2) contradicted the purpose of the subsection and did not seem to serve a purpose similar to that of the use exemption in subsection (a)(3).

Subsection (b) criminalized attempts and conspiracies to commit the offenses described in subsection (a) of the 1984 Act.[95] Subsection (b)(1) prohibited attempted violations of subsection (a).[96] In addition, subsection (b)(2) made it an offense to conspire to commit an offense under subsection (a) of the Act.[97] The conspiracy provision was patterned after the criminal conspiracy provisions in other legislation. Thus, the language of the subsection probably was meant to impose a standard equivalent to the "overt act" requirement embodied in comparable criminal provisions.[98]

Subsection (c) set penalties for convictions under the 1984 Act.[99] The subsection used a two-tier approach, imposing a lighter range of penalties for first-time offenders and applying heavier penalties for repeat offenders.[100] First-time offenders under subsection (a)(1), which prohibited unauthorized access to classified defense, foreign relations, and nuclear information, could be fined up to ten thousand dollars or

90. *See id.* at 21-22, 26-27.
91. *See id.* at 22, 26-27.
92. *See infra* note 108.
93. *See* H.R. REP. No. 894, *supra* note 66, at 21-22.
94. *Id.*
95. 1984 Act, *supra* note 17, § 1030(b) (current version at 18 U.S.C. § 1030(b) (1988)).
96. *Id.* § 1030(b)(1) (current version at 18 U.S.C. § 1030(b)(1) (1988)).
97. *Id.* § 1030(b)(2) (current version at 18 U.S.C. § 1030(b)(2) (1988)).
98. *See* Tompkins & Mar, *supra* note 22, at 469.
99. 1984 Act, *supra* note 17, § 1030(c) (current version at 18 U.S.C. § 1030(c) (1988)).
100. *Id.*

twice the value obtained by the offense, or imprisoned for up to ten years, or both.[101] Repeat offenders under subsection (a)(1) could be fined up to one hundred thousand dollars or twice the value obtained by the offense, or imprisoned for up to twenty years, or both.[102]

Similarly, first-time offenders under subsections (a)(2) and (a)(3), which prohibited unauthorized access to financial or consumer reporting agency files and misuse of government computers, could be fined up to five thousand dollars or twice the value obtained or loss created by the offense, or imprisonment up to one year, or both.[103] Repeat offenders could be fined up to ten thousand dollars or twice the value obtained or loss created by the offense, or imprisonment up to ten years, or both.[104]

Finally, subsection (d) delineated the government's investigative jurisdiction under the 1984 Act.[105] In addition, an enacted but uncodified provision of the 1984 Act stipulated that the Attorney General was to report prosecutions under the Act to Congress annually during the first three years following the statute's enactment.[106]

B. Criticism of the Original Legislation

Although leaders in the computer industry hailed the 1984 Act as an important first step,[107] legislators and industry members generally agreed that it was incomplete.[108] Many legislators and industry analysts felt that the Act needed to be expanded to protect private sector computers used in interstate commerce.[109] Moreover, state and federal law enforcement officials criticized the 1984 Act as structurally flawed and

---

101. *Id.* § 1030(c)(1)(A) (current version at 18 U.S.C. § 1030(c)(1)(A) (1988)).

102. *Id.* § 1030(c)(1)(B) (current version at 18 U.S.C. § 1030(c)(1)(B) (1988)).

103. *Id.* § 1030(c)(2)(A) (current version at 18 U.S.C. § 1030(c)(2)(A) (1988)).

104. *Id.* § 1030(c)(2)(B) (current version at 18 U.S.C. § 1030(c)(2)(B) (1988)).

105. *Id.* § 1030(d) (current version at 18 U.S.C. § 1030(d) (1988)).

106. *See* 1984 Act, *supra* note 17, § 2103 (current version at 18 U.S.C. § 1030 note (1988)).

107. *See* Betts, *Recent Computer Crime Legislation Viewed as First Step*, COMPUTERWORLD, Oct. 22, 1984, at 11.

108. *See id.* The 1984 Act was approved on October 11, 1984, as a part of the Comprehensive Crime Control Act of 1984. The Comprehensive Crime Control Act was appended to the Continuing Appropriations Resolution, House Joint Resolution 648, which was approved as public law 98-473 on October 12, 1984. The bill embodying the 1984 Act, H. R. 5616, probably would have died on Senator Paul Laxalt's desk. Representative William Hughes, the House sponsor of the bill, however, insisted as a prerequisite to compromise on the budget resolution that the Senate adopt the House-passed computer crime bill. This maneuver resulted in a compromise between House sponsors and Senate opponents in which the sponsors agreed to cut the provisions of the bill that protected computers used in interstate and foreign commerce. The compromise was for the benefit of Senator Laxalt, chairman of the Senate Subcommittee on Crime, who wanted to study the issue more carefully during the following year. *Id.*; *see also Computer Fraud Hearing*, *supra* note 22, at 1 (statement of Sen. Paul Laxalt).

109. Betts, *supra* note 107, at 11.

difficult to use.

The Justice Department had a number of criticisms of the 1984 Act.[110] It characterized subsection (a)(1), which prohibited unauthorized persons from obtaining classified data, as "largely redundant and unnecessary" because other statutes already proscribed the unauthorized possession or retention of the same information and provided for the same or harsher penalties, regardless of whether a computer was used.[111] The Department also stated that prosecutors rarely would use subsection (a)(1) because it had a higher *scienter* requirement than other applicable espionage laws.[112]

The Justice Department also criticized the scope of subsection (a)(2), which protected certain financial and credit records from unauthorized access. This subsection protected only a very narrow class of financial and credit information because it depended on the terms of the Right to Financial Privacy Act of 1978 and the Fair Credit Reporting Act.[113] By limiting the scope of protection to financial information encompassed by the Right to Financial Privacy Act, subsection (a)(2) prohibited only unauthorized access to a bank's computer to obtain information contained in the account of an individual or a partnership of five or fewer persons.[114] As a result, the subsection gave no protection to corporate accounts or to the bank's own records of its deposits in other institutions or loans because such records were not protected by the Right to Financial Privacy Act.[115] Similarly, by limiting the protection of credit information under subsection (a)(2) to the scope of the Fair Credit Reporting Act, the subsection protected only individuals and failed to protect corporate credit files.[116]

The Justice Department saw no justification for limiting protection of computerized financial and credit information to such a narrow class of data and, thus, recommended that the scope of the subsection be extended to protect all financial and credit data, personal or other-

---

110. *See Computer Fraud Hearing, supra* note 22, at 25-38 (statement of Victoria Toensing, Deputy Assistant Attorney General, Criminal Division, Department of Justice). The Justice Department's criticisms and suggestions were derived from its preparation of an administration sponsored bill (S. 1678, 99th Cong., 1st Sess. (1985)). *Id.* at 24.

111. *Id.* at 30.

112. *Id.* at 25. Section 1030(a)(1) required that a defendant knew that the protected information "[was] to be used" to harm the United States or to help a foreign nation. Other espionage statutes require only that the prosecutor prove that the defendant had "a reason to believe that the information could be used" to harm the United States or to the advantage of a foreign country. *Id.*

113. *Id.* at 31.

114. *Id.*

115. *Id.*

116. *Id.*

wise.[117] The Department added, however, that if the goal of subsection (a)(2) was to protect against the use of computers to obtain the type of personal information that was made confidential through the operation of federal laws, then the subsection should be extended to protect other types of personal data such as tax return and census information.[118]

The Justice Department also counseled modification of subsection (a)(3), which made it an offense to use, modify, destroy, or disclose information in, or to prevent authorized use of a computer operated for or on behalf of the United States if such conduct would affect the government's use of the computer. The Department recommended that the subsection should be a strict trespass provision.[119] The subsection, as formulated, proscribed unauthorized access only if the trespasser used, modified, destroyed, or disclosed data contained in government computers, or prevented authorized use of the computers.[120] The Department felt that unauthorized access to a government computer was analogous to physical trespass onto government property and recommended that prosecutors should not be required to show any additional elements, such as destruction of information, to gain a conviction.[121]

The Justice Department also saw ambiguity in another jurisdictional element of subsection (a)(3), which prohibited certain conduct only if the computer involved was operated for or on behalf of the United States government and "such conduct affect[ed] such operation."[122] The Department stated that from a grammatical standpoint the provision required the government to prove that the person's conduct affected the operation of the *computer*.[123] The Department was concerned, however, that the provision might be interpreted instead to require the prosecutor to prove that the prohibited conduct affected the operation of the *government*.[124]

The Justice Department also recommended that legislators add two new offenses and one new sanction to any future amendment of the 1984 Act. The Department suggested the additions of a computer fraud offense,[125] a destruction of property offense,[126] and a criminal forfeiture

---

117. *Id.*

118. *Id.*

119. *Id.* at 32.

120. *See* 1984 Act, *supra* note 17, § 1030(a)(3) (current version at 18 U.S.C. § 1030(a)(3) (1988)).

121. *See Computer Fraud Hearing, supra* note 22, at 32.

122. 1984 Act, *supra* note 17, § 1030(a)(3) (current version at 18 U.S.C. § 1030(a)(3) (1988)).

123. *See Computer Fraud Hearing, supra* note 22, at 32; *see also supra* Part II(A)(2) (suggesting that the House Report requires a similar interpretation of the provision).

124. *See Computer Fraud Hearing, supra* note 22, at 32.

125. *Id.* at 34.

126. *Id.* at 37.

provision.[127]

The Justice Department sought its alternative computer fraud provision due to worries that the use of a computer to facilitate the commission of a common-law offense like theft or embezzlement might prevent the application of existing federal statutes to such acts.[128] To combat that possibility, the Department recommended that legislators enact a fraud offense modeled after the federal mail and wire fraud statutes.[129] The Department further recommended that federal jurisdiction should attach to such an offense if the computer involved was owned or operated on behalf of the federal government or a federally insured financial institution, or if the offense involved computers located in two or more states or in a state and a foreign country.[130]

The Justice Department also wanted legislators to add a felony offense prohibiting the willful and unauthorized destruction of a computer owned by or operated for the government or a federally insured financial institution, or a computer program or data contained in such a computer.[131] The Department cited a clear federal interest in protecting such a limited class of computers, software, and data and concluded that such a provision would have a minimal impact on an area of jurisdiction traditionally reserved for the states.[132]

The Justice Department's final recommendation to legislators was the addition of a new punishment provision by which a defendant could be forced, upon conviction, to forfeit ownership interest in any computer used to commit an unauthorized access offense, computer fraud offense, or computer destruction offense.[133] The Department felt that a

---

127. *Id.*

128. *See id.* at 35 (describing instances in which federal prosecutors were able to adapt existing statutes to apply to computer facilitated crimes, but pointing out how such crimes would not have fallen within the purview of federal law if the facts in each case had been slightly different).

129. *Id.* at 35. The commerce clause, federal regulation, and federal insurance of many types of financial institutions would justify federal jurisdiction over such a fraud offense. *Id.* at 34.

The Justice Department emphasized that in fraud cases the computer was merely a vehicle, comparable to the mails or interstate telephone wires. Thus, the Justice Department recommended that the language of the proposed computer fraud provision track the language of existing mail and wire fraud statutes so that the "extensive body of case law that ha[d] been developed with respect to these statutes c[ould] be applied." *Id.* at 35-36.

130. *Id.* at 36. A two-state diversity jurisdictional provision "would reserve federal jurisdiction for those cases where it [was] most needed and for those which the states [would be] the least capable of investigating and prosecuting." *Id.* The Justice Department suggested that it would be unrealistic to expect a state to investigate and prosecute a fraud scheme that made use of computers located in several different states because a state's laws apply only within its borders. *Id.* Moreover, a diversity jurisdiction provision would be much less of an intrusion into states' rights than a provision that extended jurisdiction to a fraud scheme involving any computer operating in or affecting interstate commerce. *Id.*

131. *Id.* at 37.

132. *Id.*

133. *Id.*

forfeiture provision would be a particularly effective deterrent for persons who otherwise might use personal computers or small business computers to gain unauthorized access to a government computer.[134] The Department stated that a forfeiture provision was justified further by the fact that courts had not in the past tended to send such offenders to jail or impose meaningful fines.[135]

Other commentators criticized the 1984 Act for failing to define its key terms.[136] Some of the words whose meanings were critical to a clear understanding of the Act had no commonly accepted legal definition.[137] Thus, Joseph B. Tompkins, Jr., the Chairperson of the ABA Criminal Justice Section Task Force on Computer Crime, suggested that potentially ambiguous terms like "access,"[138] "authorization," "affects," and "use"[139] be defined in any amendment of the 1984 Act.[140]

Chairperson Tompkins also noted that the 1984 Act did not define "access without authorization" or give any method for determining how far "access with authorization" extended.[141] The terms were not particularly problematic in the case of hackers, but became ambiguous when applied to employees who otherwise were not trespassing on their employer's premises.[142] The legislative history of the 1984 Act made clear that subsection (a)(2) was not intended to prohibit access for a legitimate purpose pursuant to express or implied authorization.[143] Congress, however, did not define "legitimate purpose." That lack of definition, coupled with the fact that subsection (a)(2) prohibited only knowingly unauthorized access, made the effectiveness of the provision dependent on the clarity or lack thereof of an employer's definition for its employees of authority and breadth of access to information.[144]

Chairperson Tompkins also recommended more substantive

---

134. *Id.*

135. *Id.*

136. *See* Tompkins & Mar, *supra* note 22, at 475.

137. *See id.* at 475-76.

138. An earlier bill, S. 240, 96th Cong., 1st Sess. (1979), defined "access" as "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network." Similar definitions of "access" have been used in many state computer crime statutes. *See* Tompkins & Mar, *supra* note 22, at 464.

139. A House Bill defined "use" as "to instruct, communicate with, store data in, or retrieve data from, or otherwise utilize the logical, arithmetic, or memory function of a computer, or, with fraudulent or malicious intent, to cause another to put false information into a computer." H.R. 1092, 98th Cong., 1st Sess. (1983). Many states have adopted this type of definition of "use" in their computer crime statutes. *See* Tompkins & Mar, *supra* note 22, at 464.

140. Tompkins & Mar, *supra* note 22, at 476.

141. *Id.* at 464.

142. *Id.* at 464-65.

143. *See* H.R. REP. No. 894, *supra* note 66, at 21.

144. *See* Tompkins & Mar, *supra* note 22, at 465.

changes to the 1984 Act. He suggested that in addition to the types of substantive changes recommended by the Justice Department, new legislation should include a provision providing civil remedies for victims of computer crime and a section dealing with the problems of concurrent jurisdiction.[145] He also suggested that the Federal Bureau of Investigation should be granted primary investigative jurisdiction because the 1984 Act covered primarily government computers and classified information.[146]

Although legislators generally agreed that expansion of the 1984 Act was indicated,[147] the extent of expansion needed remained unclear. Legislators continued to frame the problem in terms of federal interest.[148] Senator Paul Laxalt, Chairman of the Senate Subcommittee on Criminal Law, viewed the problem as a question of how Congress intended to treat acts that were neither matters of clear federal interest nor matters clearly belonging under state and local control.[149] The Senator felt that Congress was justified in making it a federal crime to gain unauthorized access to or to damage or destroy computers and their software or data owned or operated by the federal government or federally insured financial institutions.[150] He also believed that the federal government had a clear interest in punishing those who obtained information from such computers without authorization.[151] The Senator believed that states should regulate the crimes of trespass, malicious mischief, and theft committed with privately owned computers if no federal interest in the computers or the information that they contained existed.[152] The Senator felt, however, that a number of possible criminal acts fell between these two poles and warranted further discussion.[153]

One of Senator Laxalt's primary concerns was whether state and

---

145. *Id.* at 477-78. Chairperson Tompkins believed that the potential negative consequences of abuse of civil remedies were outweighed by the severe economic impact of computer crime and the lack of other available remedies and scarcity of law enforcement resources. *Id.* at 477.

146. *Id.* at 480.

147. *See Computer Fraud Hearing, supra* note 22, at 1 (statement of Sen. Paul Laxalt).

148. *Id.* at 2.

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.*

153. *Id.* The Senator outlined three areas of concern: (1) crimes committed with computers owned by the federal government and by federally insured financial institutions; (2) crimes involving exclusively private computers that contain information with a significant federal interest, such as information protected by the Fair Credit Reporting Act; and (3) crimes involving private computers that cannot be investigated and prosecuted practically by state and local authorities even though no clear federal interest in either the computers or the data is present. *Id.*

The Justice Department criticism discussed in Part II(B) of this Note addresses the first two of these concerns. *See supra* notes 110-35 and accompanying text.

local prosecutors would be able to investigate and prosecute computer crimes that the federal government might decline to pursue.[154] William G. Petty, a representative of the National District Attorney's Association, agreed with that concern.[155] Mr. Petty felt that jurisdictional problems necessitated a preemptive federal statute because the rules of venue posed a potentially debilitating problem for state and local prosecutors.[156] He explained that unauthorized computer access often originates from remote computers through the use of telephone lines rather than through direct physical access of the target computer.[157] He also noted that a computer system subject to such access might be physically located in several different jurisdictions and that it was often difficult, if not impossible, to determine where the unauthorized access occurred.[158] He pointed out that because a prosecutor must prove that an alleged offense occurred in the jurisdiction of prosecution, many computer crimes could present a situation in which a state's attorney would be unable to prosecute in any jurisdiction in the state.[159]

Mr. Petty felt that a preemptive federal computer crime statute was preferable for a number of other reasons. He felt that the federal government's superior investigative resources were needed to combat computer related crime effectively.[160] He noted that computer related crimes often were difficult to detect and prosecute and that local law enforcement agencies often did not have the training and experience to conduct such investigations.[161] He believed that local law enforcement agencies could not commit the resources necessary to deal effectively with these types of crimes and still fulfill their obligations to respond to ordinary offenses, particularly in light of the fact that such investigations might involve a number of law enforcement agencies in a number of states.[162] Consequently, he favored preemptive federal legislation that would allow a single agency to conduct and coordinate such investigations and would make available sufficient resources to ensure successful prosecution.[163]

Mr. Petty added that a preemptive federal statute also would pro-

---

154. *Computer Fraud Hearing, supra* note 22, at 2 (statement of Sen. Paul Laxalt).

155. *Id.* at 39-50 (statement of William G. Petty on behalf of the National District Attorney's Association). Mr. Petty also served as Commonwealth Attorney for Lynchburg, Virginia at the time he testified.

156. *Id.* at 41-42.

157. *Id.*

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.*

163. *Id.*

vide a uniform definition of criminality,[164] which would be needed because no uniform definition of criminal conduct in the use of computers existed[165] Furthermore, he felt that this lack of uniformity was a distinct problem in an era in which businesses and financial institutions no longer were constrained by state boundaries because such entities need certainty that computer crimes will be penalized regardless of the state in which they occurred.[166]

Mr. Petty also admonished the legislators to be certain that any amendments to the 1984 Act were sufficiently flexible to accommodate the changing nature of computer crime and, like the Justice Department, recommended the adoption of fraud language patterned after existing federal mail and wire fraud statutes[167] because such legislation would be fiexible enough to withstand advances in technology. He warned against a "patchwork" approach of addressing specific incidents only after they had been exposed by an outrageous, yet legal, act because such an approach caused rigidity that could lead only to ineffective and obsolete legislation.[168]

Thus, Congress received a clear message that the 1984 Act needed to be expanded and clarified in a number of ways. In addition, commentators had presented numerous options for achieving these results. Jurisdiction could be broadened by expanding the types of computers protected by the Act, by expanding the types of information protected by the Act, or by making the use of computers for specified purposes unlawful, regardless of whether such use was authorized. Clarity could be improved by modifications of language and structure and by adding new definitions. Congress attempted to address these issues in the Computer Fraud and Abuse Act of 1986.[169]

---

164. *Id.* at 43.

165. *Id.*

166. *Id.* at 43-44. Although Mr. Petty favored a preemptive federal statute, he helieved that no statute would be an effective deterrent without victim cooperation. He felt that a pervasive federal statute was needed to gain the full cooperation of victims of computer crime and that such confidence would not be present unless prosecutors were able to investigate computer crimes successfully and gain the convictions of offenders, regardless of their location. *Id.* at 44.

167. *Id.*

168. *Id.*

169. 1986 Act, *supra* note 25 (codified as amended at 18 U.S.C. § 1030 (1988)).

III. The Computer Fraud and Abuse Act of 1986: A Measured Response to Criticism of the 1984 Act

A. Summary of the Changes under the 1986 Act

The amendments embodied in the 1986 Act improved the 1984 Act in a number of respects. The amendments eliminated some ambiguous language, structured the offenses more coherently, defined additional terms, and expanded the scope of the Act to encompass additional significant types of computer crime.[170]

1. Modification of the Original Provisions

The 1986 Act made seven important changes to the 1984 Act. First, the 1986 Act clarified subsections (a)(1) and (a)(2) by eliminating the convoluted "or having accessed a computer with authorization . . ." language in favor of the more succinct phrase "or exceeds authorized access."[171] Second, the 1986 Act modified subsection (a)(3) into a strict trespass provision by making unauthorized access alone a criminal offense.[172] Third, the 1986 Act repealed the use exemption that had limited the application of subsections (a)(2) and (a)(3).[173] Fourth, the 1986 Act removed a potential concern that subsection (a)(3) might discourage those seeking to expose government wrongdoing by deleting a proviso in the subsection that prohibited "disclosure" of information.[174] Fifth, the 1986 Act changed the intent requirement of subsections (a)(2) and (a)(3) from "knowingly" to "intentionally."[175] Sixth, the 1986 Act eliminated the special conspiracy provision created in the 1984 Act.[176] Finally, the specific fines set forth in the 1984 Act were repealed and replaced with the instruction that fines levied under the Act were to be imposed under "this title."[177]

2. Addition of New Provisions

The 1986 Act also expanded the reach of the 1984 Act by adding three new crimes embodied in the new subsections (a)(4), (5), and (6). Subsection (a)(4) created a federal computer fraud offense.[178] Subsection (a)(5) created an offense for the alteration, damage, or destruction

170. *See* Tompkins & Ansell, *supra* note 22, at 32.
171. 1986 Act, *supra* note 17, § 2(c), 18 U.S.C. § 1030(a)(1), (2) (1988).
172. *Id.* § 2(b)(1), 18 U.S.C. § 1030(a)(3).
173. *Id.*, 18 U.S.C. § 1030(a)(3).
174. *Id.*, 18 U.S.C. § 1030(a)(3).
175. *Id.* § 2(a)(1), 18 U.S.C. § 1030(a)(2), (3).
176. *Id.* § 2(e).
177. *Id.* § 2(f), 18 U.S.C. § 1030(c).
178. *Id.* § 2(d), 18 U.S.C. § 1030(a)(4).

of information contained in a "Federal interest computer" and prohibited the prevention of authorized use of such data.[179] In addition, subsection (a)(6) made it a crime to traffic in computer passwords under certain circumstances.[180] The 1986 Act also added a much needed definition section.[181]

B. Analysis of the Amendments Provided in the 1986 Act

The amendments to the 1984 Act left subsection (a)(1) essentially unchanged. The only change was to replace the complex and confusing "or having accessed a computer with authorization . . ." language with the simpler phrase "or exceeds authorized access."[182]

The 1986 amendments changed the *scienter* requirement in subsection (a)(2) from "knowingly" to "intentionally" and deleted the subsection's reference to the Right to Financial Privacy Act of 1978.[183] The legislators changed the *scienter* requirement for two reasons. First, they wanted to proscribe only intentional acts of unauthorized access and not mistaken, inadvertent, or careless acts.[184] Second, they felt that a "knowing" standard was inappropriate in light of the unique circumstances in cases involving computer technology.[185]

A House Report on the Criminal Code[186] stated that a person was acting knowingly if the person was cognizant that a certain result was almost certain to follow from particular conduct, whether or not that result was intended.[187] The report expressed fear that a "knowing" standard could impose liability on a person who inadvertently accessed another person's computer file or data.[188] The Senate felt that this concern was particularly justified when an individual authorized to sign on and use a particular computer subsequently exceeded authorized access by mistakenly entering another computer file or data accessible from the same terminal.[189] Legislators chose to substitute an "intentional" standard to focus federal criminal prosecutions on those persons whose

---

179. *Id.*, 18 U.S.C. § 1030(a)(5).
180. *Id.*, 18 U.S.C. § 1030(a)(6).
181. *Id.* § 2(g), 18 U.S.C. § 1030(e).
182. *Id.* § 2(c), 18 U.S.C. § 1030(a)(1).
183. *Id.* § 2(a)(1), (2), 18 U.S.C. § 1030(a)(2).
184. *See* S. REP. No. 432, *supra* note 10, at 5.
185. *Id.*
186. HOUSE COMM. ON THE JUDICIARY, CRIMINAL CODE REVISION ACT OF 1980, H.R. REP. No. 1396, 96th Cong., 2d Sess. (1980).
187. *Id.* at 33 (quoting United States v. United States Gypsum Co., 438 U.S. 422, 445 (1978)).
188. *See* S. REP. No. 432, *supra* note 10, at 6.
189. *Id.* The report explained that because a user had signed onto a terminal "knowingly," liability might be found for accidentally accessing another file because a trier of fact could infer that the user was almost certain such mistaken access could result from the initial decision to access the computer. *Id.*

conduct indicated a clear intent to access another person's computer files or data without proper authorization.[190]

The 1986 Act also modified subsection (a)(2) by deleting its reference to the Right to Financial Privacy Act of 1978.[191] The Right to Financial Privacy Act of 1978 had been used to define the terms "financial institution" and "financial record."[192] The amended Act defined these terms internally in a new subsection (e).[193] The premise of the original subsection (a)(2) was to protect, for privacy reasons, the computerized credit records and computerized information relating to customers' relationships with financial institutions.[194] Congress wanted to extend the same privacy protection to the financial records of all customers of financial institutions, including individuals, partnerships, or corporations.[195] To accomplish this aim, Congress redefined the terms "financial institution" and "financial record" in broader terms than those provided by the Right to Financial Privacy Act of 1978.

The Justice Department had been concerned that the "obtains information" language in subsection (a)(2) might require the prosecution to prove the physical removal of data as an element of the crime.[196] The Senate report clarified that subsection (a)(2)'s prohibition against obtaining information covered the "mere observation of the data" contained in such files, emphasizing again that the premise of the subsection was privacy protection.[197]

The 1986 Act replaced the original subsection (a)(3) with an entirely new provision.[198] This new provision prohibited acts of simple trespass against computers belonging to, or being used by or for, the federal government.[199] The new subsection (a)(3), however, limited the trespass offense to cases in which the offender was not employed by the federal government and had no authority to access a computer of any agency or department of the United States, or to cases in which a fed-

---

190. *Id.*

191. 1986 Act, *supra* note 25, § 2(a)(2), 18 U.S.C. § 1030(a)(2) (1988).

192. 1984 Act, *supra* note 17, § 1030(a)(2) (current version at 18 U.S.C. § 1030(a)(2) (1988)).

193. 1986 Act, *supra* note 25, § 2(g), 18 U.S.C. § 1030(e) (1988). For the text of subsection (e), see *infra* note 254.

194. *See* S. REP. No. 432, *supra* note 10, at 6.

195. *Id.*

196. *Id.*

197. *Id.* at 6-7.

198. *Compare* 1984 Act, *supra* note 17, § 1030(a)(3) *with* 1986 Act, *supra* note 25, § 2(b)(1), 18 U.S.C. § 1030(a)(3) (1988).

199. *See* S. REP. No. 432, *supra* note 10, at 7. The Justice Department had been concerned that the original subsection (a)(3) seemed to require that the prosecutor prove more than simple access. *See supra* notes 119-25 and accompanying text. Apparently Congress had not meant to require prosecutors to prove any elements beyond simple trespass. *See* S. REP. No. 432, *supra* note 10, at 7.

eral employee's act of trespass was interdepartmental in nature.[200]

Congress inserted these limitations to ensure that the subsection was not broad enough to create a risk that federal employees and others who were authorized to use a federal computer would be prosecuted for acts of computer access and use that, while objectionable, did not rise to the level of criminal conduct.[201] Congress balanced this concern against the legitimate desire to protect government computers against abuse from outsiders.[202] Congress reconciled these competing concerns by formulating the language of the subsection so that acts by government employees who merely exceeded their authorized access to computers in their own department would not be criminal.[203] The legislators felt that employees who were authorized to use a particular computer in one department, and who briefly exceeded their authorized access by improperly examining intradepartmental data, should be subject to administrative proceedings rather than criminal sanctions.[204] Congress wanted to avoid a situation in which an employee could face criminal prosecution for even the slightest unauthorized use of a departmental computer or departmental computer files.[205] Congress also saw the exclusion of this sort of activity from criminal sanctions as a means to alleviate concerns that the Act could be used to prosecute government whistleblowers.[206]

In contrast, the subsection did criminalize acts by which governmental employees gained unauthorized access to computers or data belonging to another department or agency.[207] Legislators considered that government employees who used their department or agency computers without authorization to gain access to data belonging to another department or agency were analogous to outsiders who attempted to access government computers.[208] Both the outsider and the extradepartmental government employee are without any authority to access or use the government's computer. Thus, Congress felt justified in providing criminal sanctions in such cases. Legislators acknowledged that this dichotomy between intra and interdepartmental access could, in rare cases, leave serious cases of intradepartmental trespass free from

---

200. S. REP. No. 432, *supra* note 10, at 8.

201. *Id.* at 7.

202. *Id.*

203. *Id.* The term "department" was defined in § 2(g)(4) of the 1986 Act. 1986 Act, *supra* note 25, § 2(g)(4), 18 U.S.C. § 1030(e)(7) (1988).

204. S. REP. No. 432, *supra* note 10, at 7.

205. *Id.*

206. *Id.* at 8, 21; *see also Hearings Before the Subcomm. on Criminal Justice of the House Comm. on the Judiciary*, 99th Cong., 1st Sess. 3-5 (1985) (statement of Allen Adler, A.C.L.U.).

207. *See* S. REP. No. 432, *supra* note 10, at 8.

208. *Id.*

criminal prosecution under subsection (a)(3).[209] They noted, however, that such serious acts might be subject to other criminal penalties.[210]

The new section also was intended to clarify Congress's intent that prosecutors need to show only that an offender's conduct affected the government's use of one of its computers or a computer operated on behalf of the government, not that the offender's conduct affected the overall operation of the government.[211] In addition, the new provision changed the *scienter* requirement of subsection (a)(3) from "knowingly" to "intentionally" for the same rationale as the change in subsection (a)(2).[212]

The new subsection (a)(4) created the first federal computer fraud offense.[213] Its legislative history emphasized an intent to penalize thefts of property by computer that occurred as a part of a scheme to defraud and emphasized that the new subsection required a showing that the use of the computer or computers in question was integral to the intended fraud.[214]

Congress chose not to pattern the computer fraud provision directly after existing mail and wire fraud statutes so that computer usage "wholly extraneous" to an intended fraud would not be punishable under the provision, which made violations a felony.[215] In addition, Congress chose to word subsection (a)(4) in a way that distinguished acts of theft using a computer from acts of computer trespass.[216] It considered theft, as a general rule, more serious than trespass and wanted to treat the offenses differently.[217] Legislators acknowledged that the loss of computer time resulting from repeated or sustained trespasses

209. *Id.*
210. *Id.*
211. *Id.* at 8-9.
212. *Id.* at 7.
213. *See supra* notes 125-30 and accompanying text.
214. *See* S. REP. No. 432, *supra* note 10, at 9.
215. *See id.* Legislators worried that if the subsection were patterned directly after existing mail and wire fraud statutes, the subsection might be used to punish an individual for "computer fraud" merely because the individual, in devising and executing a scheme to defraud, used a computer to keep records or calculate his potential take from the crime. Legislators felt that a fraud scheme should not fall under the scope of subsection (a)(4) merely because the perpetrator signed onto a computer at some time near the commission of the fraud. *Id.*
216. *Id.* Legislators noted that any act of trespass could be classified as a theft of property for two reasons. First, by intentionally trespassing into someone's computer files, the offender would obtain, at the least, information on how to break into that computer or system. Similarly, every trespass necessarily involves a theft of computer time. *Id.* at 9-10.
217. *Id.* at 9-10; *see also* 1986 Act, *supra* note 25, § 2(d), 18 U.S.C. § 1030(c) (1988). A first-time trespass offense would be a misdemeanor under the 1986 Act, whereas the computer fraud offense would be a felony. A trespass could, however, constitute a felony under subsection (a)(1) because mere unauthorized access of a computer containing classified data would result in the trespasser obtaining classified information in the form of knowledge concerning how to access the system itself.

could reach a level sufficient to warrant federal prosecution,[218] but believed that such acts would be punished more appropriately under a provision relating to the prevention of unauthorized use of a computer.[219] Consequently, they fashioned subsection (a)(4) to require the prosecutor to prove that the defendant accessed the computer with an intent to defraud, that the unauthorized access furthered the intent to defraud, and that the perpetrator intended to or did obtain something of value other than the use of computer time.[220]

The new felony created by subsection (a)(4) only encompassed cases involving "Federal interest computer[s],"[221] which were defined in new subsection (e)(2). Congress patterned the *scienter* requirement for the subsection, "knowingly and with intent to defraud," after the federal credit card fraud statute.[222]

Subsection (a)(5) created an offense for the intentional,[223] unauthorized alteration, damage, or destruction of information contained in a federal interest computer and for the intentional, unauthorized obstruction of use of federal interest computers or of the data they contain.[224] This subsection, like the new subsection (a)(3), was created primarily to deter activity by outsiders.[225] Subsection (a)(5) created federal protection against such outsider activity in two circumstances: (1) when any such activity caused loss to a victim or victims totalling one thousand dollars or more during any single year period;[226] and (2) when such activity involved data related to medical treatment, regardless of the amount of damage caused.[227]

Legislators decided that the one thousand dollar threshold was needed to prevent felony charges against every person who committed such acts,[228] noting that misdemeanor charges would remain available in many instances in which the threshold amount could not be proven.[229] The legislative history indicates that the concept of loss embodied in the subsection would allow recovery of expenses relating to

---

218. *See* S. REP. No. 432, *supra* note 10, at 10.

219. *See* 1986 Act, *supra* note 25, § 2(d), 18 U.S.C. § 1030(a)(5) (1986) (prohibiting this type of activity); *see also infra* notes 223-40 and accompanying text.

220. *See* S. REP. No. 432, *supra* note 10, at 10.

221. 1986 Act, *supra* note 25, § 2(d), 18 U.S.C. § 1030(a)(4) (1988).

222. *See* S. REP. No. 432, *supra* note 10, at 10 (citing 18 U.S.C. § 1029 (1988)).

223. *See id.* The "intentional" standard was intended to have the same meaning as the "intentional" standard used in subsections (a)(2) and (a)(3).

224. 1986 Act, *supra* note 25, § 2(d), 18 U.S.C. § 1030(a)(5) (1988).

225. *See* S. REP. No. 432, *supra* note 10, at 10.

226. 1986 Act, *supra* note 25, § 2(d), 18 U.S.C. § 1030(a)(5)(A) (1988).

227. *Id.*, 18 U.S.C. § 1030(a)(5)(B).

228. *See* S. REP. No. 432, *supra* note 10, at 10.

229. *Id.* at 11 (noting that the misdemeanor penalties provided in subsections (a)(2) and (a)(3) often would apply in such cases).

lost computer time,[230] reprogramming or restoring data to its original condition,[231] and certain network communications users' fees.[232] The legislative history also indicates that the losses sustained by authorized users of computer services who rely on data that has been altered can be included in reaching the one thousand dollar threshold.[233]

The legislative history precludes liability for damage caused by authorized repairs or the automatic termination devices employed by some computer leasing services.[234] Congress feared that any alteration of data caused by authorized repairs might constitute a technical violation of the subsection.[235] The Senate report, however, emphasized that the Act intentionally omitted such activity by making "unauthorized access" a prerequisite to liability.[236] Similarly, computer leasing services that employ automatic termination devices triggered by nonpayment of users' fees would not be liable under the subsection for "prevent[ing] authorized use" because users who failed to make timely payment of their fees no longer would be "authorized users."[237]

The second subsection, (a)(5)(2), created criminal liability for the alteration, damage, or destruction of medical records and required no showing of pecuniary loss on the part of any person.[238] Congress felt that the act of tampering with computerized medical records was serious enough to warrant punishment without a showing of any loss.[239] The legislative history specifies that prosecutors would not be required to show that a patient had been given an incorrect or harmful treatment because of altered medical records because the potential for such harm was sufficient to warrant criminal sanctions.[240]

Subsection (a)(6) created the last of the three new offenses in the 1986 Act. The subsection made it a crime to traffic in computer pass-

230. *See id.* The Senate report recognized the inherent value of computer time. The report pointed out that an unauthorized user could impose substantial costs on a computer service provider solely by monopolizing one channel of access to the service. *Id.* Blocking a channel of access would be one way of committing the subsection (a)(5) offense of preventing the authorized use of a computer. Thus, subsection (a)(5) covers acts of trespass involving primarily the loss of computer time that are excluded from subsection (a)(4).

231. *Id.*

232. *See id.* at 11-12. Victims also could recover losses caused by excessive communication access fees generated by the auto-dialers that hackers use in conjunction with modems when they attempt to break into computer systems that are hooked into telecommunications networks. *Id.*

233. *Id.* at 12.

234. *Id.*

235. *Id.*

236. *Id.*

237. *Id.*

238. *Id.*

239. *Id.*

240. *Id.*

words under certain circumstances.[241] Congress added the provision primarily to deter hackers from trading computer passwords over "pirate bulletin boards."[242] The subsection permitted prosecution of persons who knowingly and with intent to defraud, trafficked in computer passwords or information[243] that would allow unauthorized access to federal government computers.[244] The provision also made it possible to prosecute persons engaged in such trafficking if it affected interstate or foreign commerce.[245] The subsection defined "trafficking" as transferring or otherwise disposing of passwords to others or obtaining control of passwords with the intent of doing so.[246]

The 1986 Act also eliminated the specific conspiracy offense from subsection (b) and made a number of changes to the punishment provisions in subsection (c).[247] Congress dropped the specific conspiracy offense created by the 1984 Act so that such conduct would be governed by the general federal conspiracy provisions contained in title eighteen.[248] Similarly, Congress amended subsection (c) to provide for fines as specified in title eighteen.[249] The 1986 Act amended the penalty provisions by adding subsection (a)(6) to the list of misdemeanor offenses and creating a new felony provision to cover the offenses created by the addition of subsections (a)(4) and (a)(5).[250] The penalty provisions retained the two-tier approach to punishing repeat offenders.[251]

The 1986 Act, in response to the criticisms of the 1984 Act,[252]

---

241. 1986 Act, *supra* note 25, § (2)(d), 18 U.S.C. § 1030(a)(6) (1988).

242. *See* S. REP. No. 432, *supra* note 10, at 13.

243. *Id.* The legislative history indicates that the term "password" did not mean only a single word that enables a person to access a computer. The term also was meant to include sets of instructions for gaining access to a computer or system.

244. 1986 Act, *supra* note 25, § 2(d), 18 U.S.C. § 1030(a)(6)(B) (1988).

245. *Id.*, 18 U.S.C. § 1030(a)(6)(A).

246. *See* S. REP. No. 432, *supra* note 10, at 13. The definition was borrowed from 18 U.S.C. § 1029 (1988), which relates to credit card offenses. *See* 1986 Act, *supra* note 25, § 2(d), 18 U.S.C. § 1030(a)(6) (1988).

247. 1986 Act, *supra* note 25, § 2(e), (f), 18 U.S.C. § 1030(b), (c) (1988).

248. *See* S. REP. No. 432, *supra* note 10, at 13 (noting that Congress considered the general conspiracy offense in 18 U.S.C. § 371 (1988) preferable to a separate, specific offense).

249. The drafters of the amendments favored the general fine provisions of the Criminal Fine Enforcement Act of 1984, 18 U.S.C. § 3623 (1988), which provided fines of up to $100,000 for misdemeanor convictions punishable by more than six months in prison and fines of up to $250,000 for felony convictions. The Act also allowed judges to fine offenders up to twice the amount of their gain or twice the amount of the loss they caused their victims, whichever amount was greater.

250. 1986 Act, *supra* note 25, § 2(f), 18 U.S.C. § 1030(c) (1988).

251. *Id.*, 18 U.S.C. §§ 1030(c). Subsections (c)(3)(A) and (B) made first-time offenses under subsections (a)(4) and (a)(5) punishable by fines and/or prison sentences of up to five years for first-time offenders and imposed fines and/or prison sentences of up to ten years for repeat offenders.

252. *See supra* Part II(B).

added a new subsection which defined several terms used in the Act. The new subsection (e) added definitions for the terms "federal interest computer," "state," "financial institution," "financial record," "exceeds authorized access,"[253] and "department of the United States."[254] The final change under the 1986 Act was the addition of subsection (f), which specifically excluded the lawful "investigative, protective, or intelligence activity" of federal, state, and local law enforcement officials from coverage under the Act.[255]

IV. Additional Policy Considerations

A lack of accurate information concerning computer crime hindered legislators who attempted to address the need for federal computer crime legislation.[256] One data processing professional compared the problem to trying to "nail[] Jell-O to the wall" because no one had

253. *See* S. Rep. No. 432, *supra* note 10, at 13. The report noted that the phrase "obtaining information" as used in the definition for "exceeds authorized access" would include the mere observation of information.

254. 1986 Act, *supra* note 25, § 2(g)(4), 18 U.S.C. § 1030(e) (1988). Subsection (e)(2) defined a "Federal interest computer:"

> [A] computer—(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or (B) which is one of two or more computers used in committing the offense, not all of which are located in the same State.

Id., 18 U.S.C. § 1030(e)(2).

Subsection (e)(3) defines a "State" to include "the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States." *Id.*, 18 U.S.C. § 1030(e)(3).

Subsection (e)(4) defines the term "financial institution:"

> (A) a bank with deposits insured by the Federal Deposit Insurance Corporation; (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank; (C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation; (D) a credit union with accounts insured by the National Credit Union Administration; (E) a member of the Federal home loan bank system and any home loan bank; (F) any institution of the Farm Credit System under the Farm Credit Act of 1971; (G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; and (H) the Securities Investor Protection Corporation.

Id., 18 U.S.C. § 1030(e)(4).

Subsection (e)(5) defines the term "financial record" as "information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution." *Id.*, 18 U.S.C. § 1030(e)(5).

Subsection (e)(6) defines the term "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." *Id.*, 18 U.S.C. § 1030(e)(6).

Subsection (e)(7) defines the term "department of the United States" as "the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5." *Id.*, 18 U.S.C. § 1030(e)(7).

255. *Id.* § (2)(h), 18 U.S.C. § 1030(f).

256. *See supra* notes 41-44 and accompanying text.

a firm idea of the parameters of the problem.[257] No one had established an accepted definition of computer crime,[258] and no accurate statistics on the incidence of computer crime had been developed.[259] Computer crime was analogous to the proverbial emperor's clothes: everybody proclaimed it was there, but no one could see it. The little extant data established that some sort of problem existed,[260] but no one had a clear idea of its nature or extent.

Thus, the 1984 Act essentially was a shot in the dark. Congress defined certain acts as criminal and set penalties for those acts. Legislators were aware that the 1984 Act provided only a working definition at best,[261] but felt that immediate action to address a perceived immediate threat was necessary.[262]

Critics stated that the 1984 Act was incomplete and ineffective,[263] and prosecutors rarely used it.[264] Commentators thus suggested that new legislation was needed to broaden the scope of federal protection in order to facilitate prosecution of computer related crimes and to encourage victims to report computer crimes.[265] They observed that the lack of prosecutions limited the deterrent value of the 1984 Act.[266] Consequently, Congress attempted to define the goals of federal computer crime legislation with greater specificity. The subsequent hearings re-

---

257. *See* Betts, *supra* note 107, at 11 (quoting Richard Cashion, Chairman of the Data Processing Management Association's Committee on Computer Crime).

258. *See Computer Fraud Hearing, supra* note 22, at 43 (statement of William G. Petty on behalf of the National District Attorney's Association). Mr. Petty noted that, at the time he spoke, no uniform definition existed of what constituted criminal conduct in the area of computer related crime. *Id.*

The lack of uniformity in state law definitions of computer crime has been attributed to the fact that state computer crime laws tend to be reactive, targeting specific crimes. *See* Nawrocki, *supra* note 2, at 14-15; *see also Computer Fraud Hearing, supra* note 22, at 49 (statement of William G. Petty).

259. *See Federal Computer Systems Protection Hearing, supra* note 41, at 22 (statement of Milton R. Wessel, General Counsel to the Association of Data Processing Service Organizations).

260. *See id.* at 18. Mr. Wessel served for 17 years as the general counsel to the Association of Data Processing Service Organizations, an organization of 560 of the best known computer service companies. He stated that his position allowed him to gauge accurately the level of computer crime in the industry. He believed that computer crime was a significant problem, but felt that the companies he dealt with did not consider the problem to be epidemic. *Id.*

261. *See supra* notes 107-09 and accompanying text.

262. *See supra* notes 48-51 and accompanying text (discussing the role that interest groups and the media played in catalyzing the legislative process).

263. *See supra* Part II(B).

264. *See supra* note 22 and accompanying text.

265. *See supra* notes 164-66 and accompanying text (discussing the statement of Mr. Petty on behalf of the National District Attorney's Association). Compare, however, Mr. Petty's explanation of the problem to that given by Mr. Bloombecker, Director of the National Center for Computer Crime Data. *See* Bloombecker, *supra* note 15, at 53.

266. *See* Bloombecker, *supra* note 15, at 53.

sulted in the Computer Fraud and Abuse Act of 1986.[267]

The modification of existing provisions and addition of new provisions served two main goals. First, the 1986 Act reaffirmed Congress's intent to limit federal computer crime law to those cases involving a compelling federal interest.[268] The new law embodied an expanded notion of federal interest, but refrained from any wholesale usurpation of state jurisdiction over computer related crime. Second, the law sought to increase the deterrent effect of the existing provisions by closing loopholes, modifying the elements of the existing offenses, and restructuring and clarifying the language in the statute.[269]

Several policy considerations supported Congress's decision to maintain significant limits on the scope of federal computer crime legislation. The decision reflected the Judiciary Committee's long-standing policy of limiting federal crimes to matters of compelling federal interest or to criminal acts that state and local governments are incapable of handling.[270] Congress wanted to encourage state and local legislators and law enforcement officials to handle computer related crime.[271] The policy also recognized the need to use scarce federal law enforcement resources efficiently.[272]

The continued desire to limit the scope of federal computer crime legislation also acknowledged the states' own interests in prosecuting computer crime.[273] The acts that constitute computer crimes are all common-law crimes; the only difference is that the perpetrators of computer crime use computers to accomplish their goals.[274] All states had general criminal statutes prohibiting these sorts of acts, but they took the lead in enacting computer crime legislation when they realized that their existing criminal statutes could not deal adequately with the demands that computer facilitated crimes put on their general criminal statutes.[275] Florida enacted the first computer crime law in the nation

---

267. 1986 Act, *supra* note 25, § 2, 18 U.S.C. § 1030 (1988).

268. *See* S. REP. No. 432, *supra* note 10, at 4.

269. *See supra* Part III(A).

270. *See Computer Crime Hearing, supra* note 33, at 28 (statement of Rep. Don Edwards, Chairman of the House Subcommittee on Civil and Constitutional Rights).

271. *Id.*; *see also* S. REP. No. 432, *supra* note 10, at 4.

272. *See Computer Crime Hearing, supra* note 33, at 28; *see also* S. REP. No. 432, *supra* note 10, at 4.

273. *See* S. REP. No. 432, *supra* note 10, at 4.

274. *See Federal Computer Systems Protection Hearing, supra* note 41, at 48.

275. *See* Comment, *Computer Crime Deterrence*, 13 AM. J. CRIM. L. 391 (1986). This Comment explains how judges had interpreted general criminal statutes to exclude computer facilitated crimes. States responded to the unfavorable judicial interpretations of their general criminal statutes by enacting specific computer crime statutes designed to overcome the inadequacies of the general criminal statutes. *Id.* at 391-92.

in 1978,[276] long before federal legislators began to address seriously the need for computer crime legislation.[277] Forty-seven states had enacted specific computer crime statutes by 1986.[278] As a result, Congress would have preempted a significant body of law by enacting broader legislation and chose instead to limit federal protection to areas of "compelling Federal interest."[279]

The lack of prosecutions under the 1984 Act hurt its deterrent value. Witnesses at the committee hearings concerning amendments to the 1984 Act attributed the lack of prosecution to the Act's narrow scope and to the difficult burdens it reportedly placed on prosecutors.[280] This criticism focused the amendment process on providing additional legal tools to enhance protection under the Act, but apparently led to the exclusion of alternate means of increasing the deterrent value of the law.

Congress approached the deterrence problem under the assumption that the beneficiaries of expanded protection would make use of the tools that had been made available to them.[281] This assumption may have severely hindered Congress's effort to increase the deterrence value of the legislation because many computer crime victims had concluded that in the short term, their self-interest was served best by not reporting computer crimes.[282] They considered reporting their losses embarrassing.[283] Victims also feared that they might incur damaging publicity if they reported computer crime losses.[284] In addition, these companies felt that prosecution of computer crime was not cost-effective because of the time required to assist prosecutors and investigators

---

276. *See Federal Computer Systems Protection Hearing, supra* note 41, at 42. Florida adopted the Florida Computer Crimes Act, Chapter 815 of the Florida State Code, in August of 1978. FLA. STAT. ANN. § 815 (West Supp. 1989).

277. Senator Abraham Ribicoff introduced the first federal computer crime bill, S. 240, 96th Cong., 1st Sess. (1979), but it died quietly in committee.

278. *See* Bloombecker, *supra* note 15, at 56-57.

279. *See* S. REP. No. 432, *supra* note 10, at 4.

280. *See supra* Part II(B).

281. *See* Bloombecker, *supra* note 15, at 53. The National Center for Computer Crime Data reported that they had only been able to locate 75 prosecutions pursuant to 38 states' computer crime laws. *Id.* Many of these laws predated federal legislation. The results of the report suggest that victims of computer crime are not reporting the crimes to law enforcement officials. The Federal Bureau of Investigation reported that their estimates indicated that only one in twenty-thousand computer criminals ever went to jail. *Id.*

282. *See id.*

283. *Id.*

284. *Id.* at 53; *see also* A. BEQUAI, TECHNOCRIMES (1987), *reprinted in part in* Bloombecker, *supra* note 15, at 63. Mr. Bequai noted that banks, out of fear of losing customer confidence, often referred discovered crimes only to their in-house security for investigation. He added that banks easily could mask their losses because of the variety of definitions and procedures available to record such losses. *Id.*

and the low probability that the defendant would make full restitution, even if it was available.[285]

The legislative history of the 1986 Act, however, indicates that Congress barely acknowledged the problem of underreporting.[286] The Senate report on the 1986 Act concluded that the most effective means of deterring computer crime was through comprehensive computer security efforts.[287] Nevertheless, the legislative material gives no indication that Congress seriously considered trying to prevent computer crime by requiring businesses or other computer operators to adopt security measures or by requiring that computer crime victims report incidents to the police.[288]

A number of facts made the consideration of these reporting options very important. Witnesses informed legislators that most computer crime was committed by insiders, not teenage hackers working from home computers.[289] As a result, Congress focused on the deterrence of white collar crime as one of the major goals of the 1984 Act.[290] Legislators viewed the economic drain caused by white collar crime as a major problem that they could address successfully.[291] They also believed that facilitating the prosecution of violators under federal computer crime legislation could and would be an effective deterrent to white collar criminals.[292]

Unfortunately, the 1984 Act failed to achieve this purpose. The lack of prosecutions under the Act effectively destroyed its deterrent value. The amendments under the 1986 Act did, without question, enhance the potential for deterrence. If, however, the deterrence problem is attributed to the reluctance of victims to report computer crimes rather than to the prosecutors' inability to convict reported violators, then the 1986 Act may not have increased actual deterrence by any sig-

---

285. Bloombecker, *supra* note 15, at 53.

286. In contrast, earlier committee reports that predated the adoption of federal computer crime legislation did acknowledge and discuss the utility of other methods of deterrence, such as computer security efforts. *See Federal Computer Systems Protection Hearing, supra* note 41. *See generally Computer Security Hearings, supra* note 33; *Computer Crime Hearing, supra* note 33.

287. *See* S. REP. No. 432, *supra* note 10, at 3.

288. *See* Betts, *Cracking Down on Computer Crime*, COMPUTERWORLD, November 25, 1985, at 56. Legislators did, as a part of the debate over the passage of The Electronic Communications Privacy Act of 1986, consider whether data communications should receive privacy protection if parties took no steps to protect such information. *Id.*

289. *See Computer Crime Hearing, supra* note 33, at 49; *see also Computer Security Hearings, supra* note 33, at 41-42.

290. *See* H.R. REP. No. 894, *supra* note 66, at 5.

291. *Id.* The House Report on the 1984 Act cited statistics indicating that Justice Department prosecutions of bid-fixing cases resulted in significantly lower building costs for federal projects. *Id.*

292. *Id.*; *see also Computer Security Hearings, supra* note 33, at 41 (analogizing the need for computer crime legislation in the 1980s to the need for securities laws in the 1930s).

nificant degree.[293]

V. Recommendations for Future Amendments

Congress should consider legislation requiring businesses and other computer operators to adopt security measures and to report any computer crimes committed against them. This type of legislation could enhance the deterrent effect of the 1986 Act significantly and would help make computers less vulnerable to computer crime by requiring computer users to develop better "guards" and "locks" for their systems. The enhanced guard or auditing capabilities that would become mandatory under such regulations also would enhance the computer operator's ability to detect computer crime. Moreover, security regulations would focus computer users' thoughts on the continuing need for effective computer security. Reporting requirements also would enhance deterrence by ensuring that known computer crimes are reported and prosecuted. A reporting requirement would complement regulations requiring reasonable and effective security measures and would help generate useful data on the incidence of computer crime and how to deter such crime most effectively.

Federal banking law provides some mechanisms for requiring financial institutions to implement such requirements. Section 1882 of title twelve requires "federal supervisory agencies"[294] to promulgate rules establishing minimum standards that banks and savings and loan associations must observe with respect to the installation, maintenance, and operation of security devices and procedures in order to discourage robberies, burglaries, and larcenies and to assist in the identification and arrest of persons who commit such acts.[295] Congress could, in future amendments to federal computer crime law, stipulate that "federal supervisory agencies" as defined in title twelve be required to study the problem of computer crime in financial institutions and to promulgate security regulations specifically relating to computer security based on

---

293. *See* Editorial, *The Real Target*, Computerworld, Feb. 27, 1989, at 20 (supporting the thesis that the 1986 Act is not being used to prosecute "insider," white collar criminals for the same reasons that were listed earlier in the text of this section).

294. 12 U.S.C. § 1881 (1988) defines a "Federal supervisory agency:"

> (1) The Comptroller of the Currency with respect to national banks and district banks, (2) The Board of Governors of the Federal Reserve System with respect to Federal Reserve banks and State banks which are members of the Federal Reserve System, (3) The Federal Deposit Insurance Corporation with respect to State hanks which are not members of the Federal Reserve System but the deposits of which are insured by the Federal Deposit Insurance Corporation, and (4) The Federal Home Loan Bank Board with respect to Federal savings and loan associations, and institutions the accounts of which are insured by the Federal Savings and Loan Insurance Corporation.

Id.

295. *See id.* § 1882(a).

that research.

Section 1882 also specifies that "federal supervisory agencies" must require banks and savings and loan associations to submit periodic reports concerning the operation of their security devices.[296] This provision apparently would allow federal supervisory agencies to require applicable financial institutions to report any detected computer crimes.[297] The appropriate financial institutions must follow such security regulations and reporting requirements or be subject to "cease and desist proceedings" under the federal Safety and Soundness Act.[298]

Federal securities laws also could be adapted to achieve similar results in the corporate arena. The securities laws would not provide any computer security standards, but the reporting requirements under federal securities law could spur corporate reports of computer crime. The Foreign Corrupt Practices Act (FCPA)[299] provides an analogy of how security law could be used to enhance corporate computer security practices. The FCPA essentially prohibits "issuers" and "domestic concerns" from bribing foreign officials.[300] The FCPA also includes an accounting provision that requires issuers to make and keep books, records, and accounts that reflect, in reasonable detail, the transactions and disposition of assets of the issuer.[301] One of the primary rationales supporting the FCPA is the view that the shareholders have a right to know about overseas activity which, although not illegal under United States law, could result in a possible loss of business to the corporation.[302] A second rationale is that investors have a right to know about management's stewardship of corporate assets.[303]

The rationale for the adoption of a computer crime reporting provision under the Securities and Exchange Act would be different because the failure to report a crime is a passive rather than an affirmative act of wrongdoing. The failure to report crime only creates corporate waste

---

296. *Id.* § 1822(b).

297. Alternatively, Congress could enact specific legislation analogous to the federal money laundering statute. *See* 31 U.S.C. § 5316 (1982 & Supp. V 1987). That statute requires banks to report cash deposits of more than $10,000. *Id.* The statute, therefore, requires banks to report certain acts that would be considered evidence of money laundering activity. Similarly, Congress could enact a statute requiring financial institutions to report evidence of computer crime uncovered by internal security measures.

298. *See* 12 U.S.C. § 1818 (1988).

299. Pub. L. No. 95-213, §§ 102-104, 91 Stat. 1494 (1977) (codified as amended at 15 U.S.C. §§ 78a, 78m, 78dd-1, 78dd-2, 78ff (1988)).

300. *See id.*; *see also* Timmeny, *An Overview of the FCPA*, 9 SYRACUSE J. INT'L L. & COM. 235, 239-41 (1982).

301. *See* Timmeny, *supra* note 300, at 240.

302. *Id.* Timmeny was a Deputy Director of the Security and Exchange Commission's Division of Enforcement at the time of the passage of the FCPA.

303. *Id.*

to the extent that it weakens the deterrence value of the law and abandons the opportunity to gain restitution. Nevertheless, such passive activity in the aggregate does result in significant loss of corporate assets to white collar criminals.

A reporting requirement would allow shareholders and potential investors to assess the validity of the choice not to report losses. Market forces and the threat of shareholder actions would force the directors of corporations to give some consideration to a corporate computer crime policy.[304] This consideration would not solve the problem, but it might enhance deterrence.[305] In addition, if corporations were required to disclose their computer crime losses in a meaningful fashion, the resulting publicity might overcome any disincentive to prosecute under existing law.[306]

The mechanisms of control provided by federal security and banking laws also provide a scope of authority that is well suited to Congress's goal of limiting computer crime legislation to areas of compelling federal interest. Those mechanisms also have been tested in practice. Thus, Congress should and can consider the propriety of requiring, via these mechanisms, businesses and other computer operators to adopt security measures and to report any computer crimes committed against them.

Congress also should consider adding civil remedies and restitution provisions to the 1986 Act. Several states already have adopted such provisions to provide victims with added incentive to report computer crimes.[307] One state even provides treble damages for harm resulting from willful and malicious conduct.[308] Congress also should consider appropriating funds to train law enforcement officials and to educate the public concerning computer crime.

The symbolic value of these provisions would be very important.[309] The law serves to educate and socialize society regarding the proper

---

304. *See* Bloombecker, *supra* note 15, at 66. TRW, Inc. recently settled out of court as the defendant in a case which alleged that the corporation had failed to take proper steps to protect the privacy of computerized information under the Fair Credit Reporting Act. *Id.* Citibank also recently settled a civil action brought by the New York Attorney General's office which alleged that the bank had provided inadequate security for its automated teller machines. *Id.* Thus, a trend may be developing to hold corporations and banks responsible for their failure to protect against computer related crime. A reporting requirement would increase this sort of pressure.

305. Such reporting requirements would be useful only if corporations were required to characterize their computer crime losses clearly. Otherwise, the cause of the losses might be camouflaged. *See id.* at 63.

306. *See supra* notes 282-85 and accompanying text.

307. *See* Bloombecker, *Computer Crime Victims Have Recourse to Novel Legal Remedies*, COMPUTERWORLD, Nov. 25, 1985, at 57.

308. Connecticut provides for treble damages. *Id.*

309. *See* Hollinger & Lanza-Kaduce, *supra* note 32, at 114.

ways to approach the use of new technology.[310] Computer theft remained a private dispute among employers and employees until computer technology began to proliferate.[311] The public dissemination of computer technology was the catalyst for federal computer crime legislation,[312] as personal computers and modems externalized the computer crime phenomenon.[313] Computer crime then became a threat to normative and institutional relationships, particularly in light of the developing "hacker ethic."[314] People in all levels of society began to use computers without a clear understanding that computer data embodied traditionally valued concepts such as privacy and property.[315] Moreover, from a forward looking perspective, children of white collar families were learning to manipulate computers in an environment providing little supervision and few established norms.[316]

The 1986 Act helped to clarify the value of concepts of property and privacy as they relate to computer technology. The law served to educate potential abusers. The challenge now is to educate users and operators on how to prevent computer crime and to convince them of the desirability of reporting such crime. If Congress does not successfully meet this challenge then it is unlikely to solve the growing problem of computer crime.

Dodd S. Griffith

310. *Id.*
311. *Id.* at 115.
312. *Id.*
313. *Id.*
314. *Id.*; *see also,* Betts, *Portrait of a Hacker,* COMPUTERWORLD, Nov. 25, 1985, at 56.
315. *See* Hollinger & Lanza-Kaduce, *supra* note 32, at 116-18.
316. *Id.* at 118.