UIC John Marshall Journal of Information Technology & Privacy Law

Volume 6
Issue 3 *Computer/Law Journal - Winter 1986*

Article 2

Winter 1986

The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem, 6 Computer L.J. 459 (1986)

Joseph B. Tompkins Jr.

Linda A. Mar

THE 1984 FEDERAL COMPUTER CRIME STATUTE: A PARTIAL ANSWER TO A PERVASIVE PROBLEM†

by JOSEPH B. TOMPKINS, JR.*
and
LINDA A. MAR**

TABLE OF CONTENTS

* Joseph B. Tompkins, Jr. is a partner in the Washington, D.C., office of Sidley & Austin and is currently serving as Chairperson of the American Bar Association Criminal Justice Section Task Force on Computer Crime.

** Linda A. Mar is an associate in the Washington, D.C., office of Sidley & Austin. The authors wish to express their appreciation for the assistance provided by Jim Kole and Lauren Freeman in preparing this Article for publication.

For almost a decade, Congress has had under consideration legislation addressing various aspects of computer-related crime. In the late 1970's, Sen. Abraham Ribicoff introduced legislation which would have made computer crime a federal criminal offense.[1] In more recent years, the number of computer crime bills introduced annually has grown,[2] but until the last days of the 98th Congress, none of the bills were adopted by either the House or the Senate.

In 1983 and 1984, however, several studies on computer crime were published by public and private organizations. These studies indicated that, while the extent of computer crime and the resulting economic losses and other social costs could not be precisely estimated, computer crime is a growing national problem, causing substantial economic losses and invasions of privacy.[3] News reports describing misuses of and intrusion into computer systems, including the unauthorized penetration of computer files containing the credit records of ninety million people, also aroused public and Congressional concern. Moreover, the available evidence demonstrated that the actual and potential abusers of computers included not only juvenile "hackers" engaging in modern day joy-riding, but also sophisticated criminals committing and concealing frauds in the millions of dollars.

On October 12, 1984, Congress enacted the first federal provisions specifically outlawing certain types of computer abuse in response to these facts and concerns. This Article examines the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984[4] (hereinafter re-

---

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

2. In the 98th Congress, more than a dozen computer crime-related bills were introduced. These included S. 2940, 98th Cong., 2d Sess. (1984); S. 2864, 98th Cong., 2d Sess. (1984); H.R. 5831, 98th Cong., 2d Sess. (1984); H.R. 5616, 98th Cong., 2d Sess. (1984); H.R. 5112, 98th Cong., 2d Sess. (1984); H.R. 4954, 98th Cong., 2d Sess. (1984); S. 2270, 98th Cong., 2d Sess. (1984); H.R. 4646, 98th Cong., 2d Sess. (1984); H.R. 4384, 98th Cong., 1st Sess. (1983); H.R. 4301, 98th Cong., 1st Sess. (1983); H.R. 4259, 98th Cong., 1st Sess. (1983); S. 1920, 98th Cong., 1st Sess. (1983); S. 1733, 98th Cong., 1st Sess. (1983); H.R. 3570, 98th Cong., 1st Sess. (1983); H.R. 3075, 98th Cong., 1st Sess. (1983); S. 1201, 98th Cong., 1st Sess. (1983); H.R. 1092, 98th Cong., 1st Sess. (1983).

In the 99th Congress, more computer crime-related bills were introduced. *See, e.g.*, S. 1678, 99th Cong., 1st Sess. (1985); S. 610, 99th Cong., 1st Sess. (1985); S. 440, 99th Cong., 1st Sess. (1985); H.R. 1001, 99th Cong., 1st Sess. (1985); H.R. 995, 99th Cong., 1st Sess. (1985); H.R. 930, 99th Cong., 1st Sess. (1985).

3. *See, e.g.*, AMERICAN BAR ASS'N, CRIMINAL JUSTICE SECTION, TASK FORCE ON COMPUTER CRIME, REPORT ON COMPUTER CRIME (1984) [hereinafter cited as ABA TASK FORCE]; AMERICAN INST. OF CERTIFIED PUB. ACCOUNTANTS, REPORT ON THE STUDY OF EDP-RELATED FRAUD IN THE BANKING AND INSURANCE INDUSTRIES (1984); PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY, COMPUTER-RELATED FRAUD AND ABUSE IN GOVERNMENT AGENCIES (1983).

4. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, § 2102, 1984 U.S. CODE CONG. & AD. NEWS (98 Stat.) 1837, 2190 (codified at 18 U.S.C. § 1030). The entire text of § 1030 is appended to this Article. As originally passed by the House, these provi-

ferred to as the Act), which was enacted as part of the Comprehensive Crime Control Act of 1984. This Article describes what the Act's provisions cover and discusses some of the problems either created or not addressed by the Act. The Article then briefly discusses potential solutions to these problems, including those contained in pending legislative proposals. The issues that are raised by the Article are merely suggestive and certainly not exhaustive.

I. DESCRIPTION AND ANALYSIS OF THE ACT

A. SUMMARY

The Act prohibits the unauthorized use or accessing of computers in three relatively narrow areas. First, the Act makes it a felony to access or use a computer without authorization to obtain classified United States military or foreign policy information with the intent or reason to believe that such information will be used to harm the United States or to benefit a foreign nation.[5] Second, the Act makes it a misdemeanor to access or use a computer without authorization to obtain financial or credit information that is protected by federal financial privacy laws.[6] Third, the Act makes it a misdemeanor to access a federal government computer without authorization and thereby use, modify, destroy, or disclose any information therein, or prevent others from using the computer, if operation of the computer is thereby affected.[7]

The Act also prohibits any attempt or conspiracy to commit any of

---

sions were part of the second half of H.R. 5616, 98th Cong., 2d Sess. (1984). The first half of that bill was enacted as the Credit Card Fraud Act of 1984 (§ 1602 of the Comprehensive Crime Control Act) and is codified at 18 U.S.C. § 1029 (Supp. II 1985). Although this article only analyzes § 1030, such access devices can also play a role in computer-related crime.

The Credit Card Fraud Act of 1984 provides for the punishment of anyone who: (1) produces, uses, or traffics in one or more counterfeit access devices; (2) traffics in or uses one or more unauthorized access devices during any one-year period, and thereby obtains anything of value aggregating $1,000 or more during that period; (3) possesses fifteen or more counterfeit or unauthorized access devices; or (4) produces, traffics in, has control or custody of, or possesses device-making equipment. These acts constitute offenses if performed knowingly and with intent to defraud and if they affect interstate or foreign commerce. 18 U.S.C. § 1029(a) (Supp. II 1985). Attempts and conspiracies to commit the offenses described are also prohibited. *Id.* § 1029(b).

An "access device" is defined as any card, plate, code, account number, or other means of account access. *Id.* § 1029(e)(1). A "counterfeit access device" is any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device. *Id.* § 1029(e)(2). An "unauthorized access device" is any access device that is lost, stolen, expired, revoked, cancelled, or obtained with intent to defraud. *Id.* § 1029(e)(3).

5. *Id.* § 1030(a)(1).
6. *Id.* § 1030(a)(2).
7. *Id.* § 1030(a)(3).

those three offenses.[8] Penalties are enhanced for repeat offenders.[9] The U.S. Secret Service is designated as having investigative authority for these provisions "in addition to any other agency having such authority."[10] The Secretary of the Treasury and the Attorney General are to enter into an agreement as to the scope of the authority of the Secret Service.[11]

B. The Legislative History

The official title of the enacted computer crime provisions—the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984—is somewhat misleading. The provisions as enacted do not even address counterfeit access devices and are not aimed directly at computer fraud. The Act's title reflects the bill as originally proposed by Rep. Hughes in H.R. 5112,[12] as amended by H.R. 5616.[13] In addition to prohibiting computer abuse, H.R. 5616 outlawed counterfeit access devices and computer fraud in interstate commerce.[14] On June 26, 1984, the House Judiciary Committee amended H.R. 5616 extensively, clarifying its coverage of classified information and adding a definition of "computer." On July 24, 1984, the House passed H.R. 5616, as amended, in its entirety.

On October 11, 1984, the Senate amended and passed H.R. 5616. At about the same time, however, the leaders of both the House and the Senate were anxious to see a number of important criminal law measures enacted before Congress adjourned. The Conference Committee agreed to include the counterfeit access device and computer abuse provisions of the House version of H.R. 5616 in the comprehensive crime control package. In so doing, the Committee omitted the computer fraud provisions of H.R. 5616. The Comprehensive Crime Control Act of 1984 was appended to the Continuing Appropriations Resolution, House Joint Resolution 648, which was approved as Public Law 98-473 on October 12, 1984. The enacted computer crime provisions, which cover only three narrow areas of unauthorized access and abuse, retained the original title of H.R. 5616.

C. Prohibited Acts

As the first federal computer crime statute, the Act is important

8. *Id.* § 1030(b)(1), (2).
9. *Id.* § 1030(c).
10. *Id.* § 1030(d).
11. *Id.*
12. H.R. 5112, *supra* note 2.
13. H.R. 5616, *supra* note 2.
14. *Id.*

not only for what it covers, but also for what it leaves open for further federal and state legislation. In this new legislative area, definitions are difficult to formulate in a manner that is neither underinclusive nor overinclusive, and in a way that can keep pace with rapid changes in technology. The provisions of the Act, while generally straightforward, leave a number of questions unanswered.

1. *Unauthorized Computer Access*

Each of the three subparagraphs of 18 U.S.C. § 1030(a) sets forth the initial jurisdictional requirement of the Act. Those subparagraphs specify that the Act applies only to anyone who "knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend . . . ."[15]

The only term defined in the statute is "computer":

> 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.*[16]

The exclusion of hand held calculators and automated typewriters reflects the Congressional concern that the Act should not apply to conduct of a *de minimis* nature. By contrast, of the states that have computer crime statutes, most do not exclude calculators and typewriters from the definition of "computer."[17]

In explaining the definition of "computer," the House Judiciary Committee observed that

> [t]he whole issue of defining the word "computer" has plagued the consideration of computer crime legislation since its early days . . . . Initially, it was the Subcommittee on Crime's opinion that the dictionary definition was as good as [sic] one available considering the volatile state of technology in this area. The Committee decided, however, that a specific definition was desirable in order to avoid attacks upon the statute on the grounds of vagueness.[18]

According to the Committee, the definition of "computer" is a combina-

15. 18 U.S.C. § 1030(a)(1).

16. *Id.* § 1030(e) (emphasis added).

17. Many of the state statutes are modeled after S. 240, *supra* note 1, which defined "computer" as "an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network."

18. H.R. REP. NO. 894, 98th Cong., 2d Sess. 23, *reprinted in* 1984 U.S. CODE CONG. & AD. NEWS 3689, 3709.

tion of the definition in H.R. 1092, a bill proposed by Rep. Nelson in 1983,[19] and a definition in S. 2940, a bill proposed by the Justice Department and introduced by Sen. Thurmond in 1984.[20] In S. 2940, "computer" was defined in essentially the same words used in the Act, but there were no exceptions in the definition.[21] H.R. 1092, in addition to excluding the same devices as the Act, excluded personal and home computers not used to access, manipulate, or communicate with another computer. It is improbable that such personal home computers were intended to fall under the Act's exclusion of "other similar devices."[22]

"Access" and "use" are not defined in the Act. The 1979 Ribicoff bill, S. 240, 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."[23] Furthermore, H.R. 1092 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."[24] These (or very similar) definitions of "access" and "use" have been employed in many state computer crime statutes. The meaning of those two terms in the Act is not clear. For example, it is unclear whether the word "use" is intended to encompass causation of another to put false information into a computer, as "use" is defined in H.R. 1092, and whether "access" is intended to have the same meaning as "access" in S. 240.

The provisions also do not define what constitutes access "without authorization" or how to determine how far access "with authorization" extends. Clearly, the typical computer hacker does not have authorization to access or use a bank or government computer. The legislative history of the Act indicates that the provisions were aimed at such "so-called computer 'hackers' who have been able to access (trespass into) both private and public computer systems, sometimes with potentially serious results."[25]

---

19. H.R. 1092, *supra* note 2.

20. S. 2940, *supra* note 2, § 2.

21. S. 1678, *supra* note 2, the new Department of Justice proposal introduced by Sen. Thurmond on September 20, 1985, contains the same definition of "computer" as did S. 2940.

22. The failure to incorporate the additional exclusions of H.R. 1092 is without practical effect, because personal home computers which lack the ability to manipulate, access, or communicate with another computer would unlikely be involved in the three types of computer crimes covered by the Act.

23. S. 240, *supra* note 1, § 3.

24. H.R. 1092, *supra* note 2.

25. H.R. REP. NO. 894, *supra* note 18, at 10, 1984 U.S. CODE CONG. & AD. NEWS at 3695.

It is less clear what Congress intended to constitute access "without authorization" or what it viewed as the scope of "authorized" access for employees who otherwise are not trespassing upon their employer's premises. In describing what was enacted as section 1030(a)(2), the House Judiciary Committee 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."[26] Thus, it would appear Congress presumed that employees have implicit or express authorization to access computers. Congress did not address, however, the issue of how one defines a "legitimate purpose." Furthermore, since the law provides that the unauthorized access be done "knowingly," effective enforcement of the law may depend in large part upon having employers clearly define for employees exactly *who* can access *what*, and state the limits imposed once authorized access occurs.[27]

If it is determined that a person has accessed or used a computer without adequate authorization, criminal liability will result if the conduct falls in any of the three categories under section 1030:

> a. *Obtaining classified defense, foreign relations, or nuclear information*: The first category of prohibited conduct is the obtaining of information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.[28]

Paragraph r. of section 11 of the Atomic Energy Act of 1954 defines "re-

---

26. *Id.* at 21, 1984 U.S. CODE CONG. & AD. NEWS at 3707 (emphasis added).

27. Some states define "unauthorized access" in their computer crime statutes and legislation. Connecticut, somewhat tautologically, provides that a "person is guilty of . . . unauthorized access to a computer system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization." CONN. GEN. STAT. ANN. § 53a-251(b)(1) (West 1985). Connecticut provides for a "causation" theory of criminal liability and an affirmative defense if the person reasonably believes that he or she *would* have received authorization without payment of consideration. *Id.* § 53a-251(b)(2). Similar provisions do not appear in the federal Act.

Under Virginia law, a person is "without authority" when he or she "has no right or permission of the owner to use a computer, or, he [or she] uses a computer in a manner exceeding such right or permission." VA. CODE § 18.2-152.2 (Supp. 1985). The Virginia statute's language probably comes closest to the meaning of the federal provisions, incorporating a provision similar to that of the Act's prohibition against "use for purposes to which the authorization does not extend."

28. 18 U.S.C. § 1030(a)(1) (Supp. II 1985).

stricted data" as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category . . . ."[29] Thus, subsection (a)(1) of section 1030 covers sensitive data concerning nuclear technology and national defense.

The language of subsection (a)(1) indicates that scienter is a requirement of this felony provision, i.e., the unauthorized conduct is criminal only if the person intends or has reason to know that the data obtained will be used to harm the United States or help another nation. This scienter requirement reflects Congress' intent to pattern the provision after the existing espionage laws.[30]

Because of the scienter requirement, there may be some "innocent" unauthorized acquisition of classified data not covered by this provision. For example, it would appear that computer hackers could simply view the classified data for their own pleasure. Moreover, this type of "trespass" would not be prohibited by subsection (a)(3) because that subsection does not apply to mere "browsing."

Like the espionage laws, subsection (a)(1) applies even if the information obtained is not intended to be used to harm the United States, but only to aid another nation, no matter how friendly.[31]

b. *Obtaining private financial information*: The second category of prohibited conduct is the obtaining of

> information contained in a financial record of a financial institution, as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).[32]

Subsection (a)(2) was added because of Congressional concern about incidents in which hackers browsed through private financial and credit files in computers, such as the intrusion into TRW's massive computer credit files in 1984.[33] This subsection reinforces the privacy of information already made confidential by federal law under the Right to Financial Privacy Act of 1978[34] and the Fair Credit Reporting Act.[35]

---

29. 42 U.S.C. § 2014(y) (1982).

30. 18 U.S.C. §§ 793-799 (1982). *See* H.R. REP. NO. 894, *supra* note 18, at 21, 1984 U.S. CODE CONG. & AD. NEWS at 3706-07. The Judiciary Committee, quoting Gorin v. United States, 312 U.S. 19, 28 (1941), stated: "This requires those prosecuted to have acted in bad faith. The sanctions apply only when scienter is established."

31. *See* Gorin v. United States, 312 U.S. 19 (1941).

32. 18 U.S.C. § 1030(a)(2) (Supp. II 1985).

33. *See* 130 CONG. REC. H6315 (daily ed. June 22, 1984) (statement of Rep. Hughes).

34. 12 U.S.C. §§ 3401-3422 (1982).

35. 15 U.S.C. §§ 1681-1681t (1982).

The terms used in subsection (a)(2) are defined in those respective Acts.[36] The House Judiciary Committee indicated that the information covered by subsection (a)(2) would generally be the same as that described in these two Acts.[37] The reach of subsection (a)(2), however, extends to *all* persons, while the Financial Privacy Act applies only to federal employees and the Fair Credit Reporting Act applies only to consumer reporting agencies.[38]

The Right to Financial Privacy Act restricts the disclosure, by a financial institution to a federal governmental agency, of records related to the financial institution's customers who are individuals or partnerships consisting of five or fewer partners.[39] It does not cover information that cannot be identified with a particular person.[40] Similarly, the Fair Credit Reporting Act protects information in credit reporting agency files.[41] Such information may concern a person's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.[42] The extensive use of computers to store and retrieve such information creates the potential for serious invasions of privacy.

Unlike subsection (a)(1), subsection (a)(2) does not include a requirement that the information be obtained with the intent to injure anyone. The only requirement beyond unauthorized access is that the person obtain the private information. Obtaining a hard copy of the information does not appear to be required to fall within the ambit of the

---

36. Under the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401(1) (1982), "financial institution" is defined 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]." "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, 15 U.S.C. § 1681a(f) (1982), defines "consumer reporting agency" as

> any 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 information 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.

"Consumer" is defined as an individual. *Id.* § 1681a(c).

37. H.R. REP. NO. 894, *supra* note 18, at 21, 1984 U.S. CODE CONG. & AD. NEWS at 3707.

38. *Id.*

39. 12 U.S.C. §§ 3401(4), 3402 (1982).

40. *Id.* § 3413(a).

41. 15 U.S.C. §§ 1681-1681t.

42. *Id.* § 1681a(d).

statutory prohibition. Apparently, "just looking" at the information is enough to violate subsection (a)(2).

If a person accesses a computer with authorization and uses that opportunity for purposes beyond authorization, then such access is *not* an offense under subsections (a)(2) or (3), "if the using of such opportunity consists only of the use of the computer."[43] The "use" exemption would seem to have no application to section (a)(2), because the requirements of (a)(2)—that one must have obtained information in statutorily-defined financial records—are very clear. If a defendant does not obtain such information, then subsection (a)(2) is inapplicable. At best, the "use" exemption, as applied to subsection (a)(2), creates an ambiguity or apparent inconsistency in the statutory language which is likely to cause unnecessary litigation.[44] In contrast, as discussed below, the "use" exemption may have direct application to subsection (a)(3), to the point where that section is largely eviscerated.[45]

c. *Abusing federal government computers*: The third category of prohibited conduct is set forth in subsection (a)(3) and covers anyone who accesses without authorization and in so doing "knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation."[46]

It is unclear what "affects such operation" means. Presumably, if one does any of the acts specified in subsection (a)(3), the operation of the government computer will be "affected." If "affects" is construed to mean that the operation of government computers must be interrupted, then the "prevents authorized use" clause would appear to be redundant. If "affects" means something less than "prevents authorized use," but something more than the literal meaning of the word, it could appear to be a significant defense to an alleged violation of subsection (a)(3). In addition, if the "use" exemption described above is liberally construed, then the circumstances under which subsection (a)(3) could be enforced would appear to be very narrow. Even if one were to "affect" the operation of a government computer by merely "using" the computer, then the obtaining of information in government computers

43. 18 U.S.C. § 1030(a) (Supp. II 1985).

44. It is possible that the "use" exemption was linked to subsection (a)(2) by mistake. Originally, H.R. 5616 provided the exemption only for what is now subsection (a)(3) and a provision that was not enacted (which would have prohibited unauthorized computer access that results in a loss to the victim or gain to the criminal of at least $5,000 per year). The intent of the exemption was to exclude "time-stealing" from the statute.

45. *See infra* text accompanying notes 46-50.

46. 18 U.S.C. § 1030(a)(3) (Supp. II 1985).

(and perhaps even the modification or destruction of such information) would seem to be beyond the scope of the Act.

An additional concern about subsection (a)(3) is its effect upon government employee "whistleblowers" who attempt to expose fraud and other abuses in government. Though the Act's drafters assured that whistleblowers would be unaffected,[47] the literal language of subsection (a)(3) appears to be applicable to whistleblower activity. Accordingly, the American Civil Liberties Union (ACLU) has expressed concern about the chilling effect on whistleblowers.[48] Senator Leahy agreed with the ACLU:

> The most serious problem with the bill as it now stands is that it makes every unauthorized disclosure of information from a Government computer a crime . . . . It makes no difference under this bill that a Government employee who has accessed the computer lawfully discloses information that is not secret or classified. It can even be information that is available under the Freedom of Information Act.[49]

The Senate has attempted to amend the Act by clarifying its application with regard to government employees.[50]

2. *Attempts and Conspiracies*

Subsection (b)(1) of the Act provides that "[w]hoever attempts to commit an offense under subsection (a) of this section" shall be subject to the penalties provided in subsection (c).[51] This section raises the usual questions surrounding what constitutes an "attempt to commit"; otherwise, subsection (b)(1) is clear and unobjectionable.

Subsection (b)(2) of the Act provides for the punishment of anyone who "is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this [Act], if any of the parties engages in any conduct in furtherance of such offense . . . ."[52] This conspiracy provision is patterned after other criminal conspiracy provisions. Thus, the phrase, "if any of the parties engages in any conduct in furtherance of such offense," probably imposes a standard equivalent to the "overt act" requirement.[53]

---

47. *See* 130 CONG. REC. H12,074 (daily ed. Oct. 10, 1984) (statement of Rep. Hughes).

48. *See Hearings Before the Subcomm. on Criminal Justice of the House Comm. on the Judiciary*, 99th Cong., 1st Sess. 3-5 (1985) (statement of Allan Adler, ACLU) [hereinafter cited as *Hearings*].

49. 130 CONG. REC. S14402-03 (daily ed. Oct. 11, 1984) (statement of Sen. Leahy).

50. The Senate amended H.R. 5616 to clarify its application to government employees, but the House did not have enough time to act upon the amended bill. In March 1985, Senator Mathias proposed a similar amendment to the Act. *See* S. 610, 99th Cong., 1st Sess., 131 CONG. REC. S2728-29 (daily ed. Mar. 7, 1985).

51. 18 U.S.C. § 1030(b)(1) (Supp. II 1985).

52. *Id.* § 1030(b)(2).

53. Some criminal conspiracy provisions specifically incorporate the "overt act" re-

D. PENALTIES

Subsection (c) of the Act sets forth a graduated scale of penalties for offenses committed under the Act. For violations of subsection (a)(1), which prohibits improper access to classified or national security information, there are two categories of sanctions: (1) for first-time offenders, a fine of up to $10,000 or twice the value obtained by the offense, or imprisonment for up to ten years, or both; (2) for repeat offenders, up to $100,000 or twice the value obtained by the offense, or imprisonment up to twenty years, or both.[54]

For violations of subsections (a)(2) and (a)(3), which prohibit improper access to financial or consumer reporting agency records and abuse of government computers, the Act again provides increased penalties for repeat offenders: (1) for first-time offenders, a fine of up to $5,000 or twice the value obtained or loss created by the offense (whichever is greater), or imprisonment up to one year, or both; (2) for repeat offenders, a fine of up to $10,000 or twice the value obtained or loss created by the offense (whichever is greater), or imprisonment up to ten years, or both.[55]

These provisions raise obvious evaluation problems, such as what is the "value" of obtaining national security information, or what "loss" is created by improper access to personal financial records? Such problems, however, are unavoidable if one attempts to make the punishment correspond to the impact of the crime; and, unfortunately, terms such as "value" and "loss" are not amenable to clear, operational definitions.

E. INVESTIGATIVE JURISDICTION AND REPORTING

Subsection (d) provides that the U.S. Secret Service has the authority to investigate offenses under the Act, "in addition to any other agency having such authority."[56] The subsection also provides that the Secret Service's authority shall "be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General."[57] Presumably, "any other agency having such authority" refers to the Federal Bureau of Investigation (FBI) and

---

quirement, while others have been interpreted to require an overt act even though their language does not state so specifically. *See, e.g.*, 18 U.S.C. § 1117 (1982) (murder) and 18 U.S.C. § 1201(c) (1982) (kidnapping) ("If two or more persons conspire . . . and one or more of such persons do any overt act to effect the object to the conspiracy . . ."); *cf.* 18 U.S.C. § 371 (1982) (defrauding the United States) ("If two or more persons conspire . . . and one or more of such persons do any act to effect the object of the conspiracy").

54. 18 U.S.C. § 1030(c)(1) (Supp. II 1985).

55. *Id.* § 1030(c)(2).

56. *Id.* § 1030(d).

57. *Id.*

implies that the Treasury-Justice agreement could provide for the sharing of investigative authority between the Secret Service and the FBI or perhaps other investigative agencies, such as the Inspectors General.

Finally, a separate provision of the Act, which was enacted but not codified, requires that the Attorney General report to Congress annually (during the first three years of the statute's existence) concerning prosecutions under the Act.[58]

II. PROBLEMS CREATED OR LEFT UNANSWERED

The Act has many commendable attributes. A number of problems, however, were left unanswered, while at the same time new problems were created. These old and new problems will be discussed in the context of the following issues—the scope of the legislation; the clarity and consistency of the legislation; remedies provided in the legislation; and the investigative and prosecutorial jurisdiction contemplated by the legislation. While many of these problems are dealt with in pending legislative proposals, some are not. The overall objective of Congress in reviewing the Act should be the enactment of comprehensive, consistent, and enforceable legislation—either through amending or replacing the Act.

A. SCOPE

As the previous discussion indicates, the Act is a narrowly defined piece of legislation which focuses on three specific areas of computer-related crime. Given the political circumstances surrounding the passage of the Act, this limited and cautious step is certainly understandable.

Congress should now, however, amend or replace the Act with legislation providing for broader jurisdiction over computer-related crimes. There are two basic reasons for doing so. First, there are computer-related "crimes" which are not directly covered by the Act or other federal laws. This may have serious consequences for the agencies, companies, or individuals affected. Examples include improper access to (or destruction of) computer records which are not covered by the narrow provisions of the Act. Second, it is clear that many of these "crimes" will not or cannot be effectively detected, investigated, and prosecuted by state and local authorities.

Federal jurisdiction could be broadened in a number of ways: (1) by expanding the types of computers covered by the Act; (2) by expanding the types of information protected by the Act; (3) by making

58. Comprehensive Crime Control Act of 1984, *supra* note 4, § 2103, 1984 U.S. CODE CONG. & AD. NEWS (98 Stat.) at 2192.

the use of computers for certain purposes unlawful, regardless of whether such use is "authorized"; and (4) by repealing any dollar thresholds necessary to trigger federal jurisdiction.

Most of the pending legislative proposals would result in broadened jurisdictional coverage.[59] H.R. 930 would do so by adding a new subsection (f) to 18 U.S.C. § 1030, providing the following:

> (f)(1) Whoever knowingly accesses a computer to which the protections of this subsection apply without authorization, or having accessed such a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby obtains property of another or modifies or destroys property of another shall be imprisoned not more than ten years or fined not more than $250,000, or both.[60]

H.R. 930 would also expand the definition of "computer" to include computers owned or operated on behalf of federally-regulated financial institutions or computers operating in or using a facility of interstate or foreign commerce. Furthermore, H.R. 930 broadly defines "property" to include "anything of value," thereby also expanding and clarifying the scope of federal jurisdiction.[61]

H.R. 1001 would broaden federal jurisdiction by adding subsections (4) and (5) to 18 U.S.C. § 1030(a), providing for the punishment of any person who:

> (4) having devised a scheme or artifice to defraud, knowingly and with intent to execute such scheme or artifice, accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of one or more instances of such conduct obtains anything of value (other than the use of the computer) aggregating $5,000 or more during any one year period, and affects interstate or foreign commerce; or
>
> (5) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of one or more instances of such conduct obtains anything, or causes a loss, of a value aggregating $5,000 or more during any one year period, and affects interstate or foreign commerce . . . .[62]

In addition to clarifying the meaning of a number of key terms, S. 440 would expand the reach of federal jurisdiction to include offenses involving a computer which "operates in, or uses a facility of, interstate

---

59. The four most prominent legislative proposals now pending before the 99th Congress are S. 1678, *supra* note 2; S. 440, *supra* note 2; H.R. 1001, *supra* note 2; and H.R. 930, *supra* note 2.

60. H.R. 930, *supra* note 2.

61. *Id.*

62. H.R. 1001, *supra* note 2.

or foreign commerce."[63] S. 440 would also add the following provision to section 1030:

> (e)(1) Whoever knowingly—
>
> (A) accesses a computer described in paragraph (4) without authorization, or
>
> (B) having accessed such a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby knowingly—(i) executes or attempts to execute a scheme or artifice to defraud; (ii) obtains or attempts to obtain the property of another; (iii) causes or attempts to cause the withholding or denial of the use of such computer; or (iv) modifies, damages, or destroys property of another.
>
> shall be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned for not more than five years, or both.[64]

S. 1678 would replace the present Act with a statute that is both broader and structurally different. That proposal would replace existing sections 1030(a) and (b) with the following language:

> (a) Whoever having devised or intending to devise any scheme or artifice to defraud or for obtaining money or property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or convert to his use or the use of another, property not his own, for the purpose of executing such scheme or artifice or embezzlement, theft or conversion or attempting to do so, knowingly obtains access to or attempts to obtain access to a computer shall—
>
> (1) if the computer is owned by, under contract to, or operated for or on behalf of—
>
> (A) the United States Government; or
>
> (B) a financial institution; or
>
> (2) if in committing or concealing the offense of [sic] two or more computers are used which are located in different States or in a State and a foreign country,
>
> be fined not more than $250,000 or imprisoned not more than five years, or both.
>
> (b) Whoever knowingly and willfully without authorization damages, destroys, or attempts to damage or destroy a computer described in subsection (a)(1) or any computer program or data contained in such computer shall be fined not more than $250,000 or imprisoned not more than five years, or both.
>
> (c) Whoever intentionally without any authorization obtains access to a computer described in subsection (a)(1) or a computer system or computer network including such computer, shall be guilty of a misde-

63. S. 440, *supra* note 2.

64. *Id.* S. 440 would also add a provision making the knowing unauthorized access to computers, as defined in the statute, a misdemeanor with a fine of not more than $5,000.

> meanor and shall be fined not more than $100,000 or imprisoned for not more than one year, or both.[65]

Section (a) of S. 1678 is patterned directly after the mail[66] and wire fraud statutes.[67]

Both H.R. 1001 and H.R. 930 are laudable for attempting to broaden federal jurisdiction. Both, however, are flawed in that they employ the "knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" language used in the present Act. Whatever its merits in the present Act, this language is likely to create significant enforcement problems and appears to be wholly unnecessary in the proposed amendments. If a computer is used to further a scheme or artifice to defraud or to take or destroy someone else's property, whether the use was authorized or not, seems to be irrelevant.

In addition, the jurisdictional requirement in H.R. 1001 of $5,000 over the period of a year and the added requirement that the use of the computer in question "affect interstate or foreign commerce" are troublesome. The dollar threshold requirement would likely create factual disputes and enforcement problems that overshadow any protection provided against federal "overreaching." The requirement that the conduct in question "affect interstate commerce" again creates a factual issue that may be difficult and costly to resolve and may unreasonably inhibit enforcement of the statute. A requirement, such as the one contained in H.R. 930, that the *computer* operate in, or use a facility of, interstate or foreign commerce, seems much more reasonable and realistic.

S. 440 seems preferable to either of the House bills, because it explicitly defines more of the ambiguous terms, and because its organization recognizes the analytical distinctions among the types of computer crime.[68] Yet, S. 440, like H.R. 930 and H.R. 1001, is also flawed. S. 440

---

65. S. 1678, *supra* note 2.

66. 18 U.S.C. § 1341 (1982).

67. 18 U.S.C. § 1343 (1982). Section 1343, for example, states:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both.

68. S. 440 enumerates four separate categories of computer crime in § 3 and separates the offense of unauthorized access from offenses involving access beyond that authorized. These distinctions, which are not made clear in the Act or in the proposed amendments contained in H.R. 930 and H.R. 1001, would aid in the interpretation and enforcement of the Act.

refers to authorization in defining crimes for which the level of authorization would seem irrelevant; yet S. 440 fails to define the word "authorization."

S. 1678 is praiseworthy for its organizational clarity and for patterning its language after the mail and wire fraud statutes. S. 1678 is also laudable, because it makes authorization, or the lack thereof, irrelevant for offenses involving the use of computers to commit fraud, embezzlement, theft, or other unlawful acts.[69] The scope of jurisdiction as defined in S. 1678, however, is objectionable in two respects. First, in order for section (a) to apply, the computer involved must either have some connection with the federal government or a financial institution, or the offense must involve two or more computers that are located in different States or in a State and a foreign country.[70] The latter requirement would exclude schemes involving computers in the same State which nevertheless may have serious effects on interstate or foreign commerce. An alternative formulation, such as that used in H.R. 930—of "operating in, or using a facility of, interstate or foreign commerce"—would seem preferable.

Second, sections (b) and (c) of S. 1678 apply only to computers as defined in (a)(1), i.e., computers owned by, under contract to, or operated for, or on behalf of the United States Government or a financial institution. Thus, privately-owned computers, even if they were in different states and used facilities of, or affected, interstate commerce, would not be protected by the destruction prohibition of section (b) or the improper access prohibition of section (c).[71] These exclusions from federal jurisdiction seem to be based on the assumptions that minor offenses will be excluded and major offenses will be handled at the state or local level. These assumptions would seem to be misplaced.

Of all the bills being considered, S. 1678 could present the most comprehensive, understandable, and effective approach to defining federal jurisdiction. A few amendments to correct the problems previously discussed would make this bill even more effective.

B. CLARITY AND CONSISTENCY

One area of concern with the present Act is the lack of definitions of key terms. The only word defined is "computer."[72] While it is unnecessary and probably inadvisable to define each significant word in

69. S. 1678, *supra* note 2.

70. *Id.*

71. S. 2940, *supra* note 2, the predecessor of S. 1678, did not restrict the application of section (b) to computers as defined in section (a)(1).

72. As indicated previously, the original version of the Act contained no definitions. The definition of "computer" was added shortly before the legislation was enacted.

the statute, it would be helpful to define those words that are critical to the interpretation of the statute and do not have commonly-accepted meanings. The words in the present Act that merit definition include: "access"; "authorization"; "use"; and "affects." Obviously, if the scope of the legislation is expanded, as suggested above, additional definitions may be necessary. Existing state computer crime statutes, as well as previously proposed federal legislation, can provide guidance for defining key terms. Each of the major pieces of pending federal legislation provides some definitions of key terms. S. 1678 is the most comprehensive in defining its terms,[73] and is preferable in that respect.

The present Act could also be improved by enhancing its internal consistency. For example, the consistency of the "affects such operation" condition at the end of subsection (a)(3) with earlier parts of that subsection should be examined. The meaning and purpose of the "use" exemption at the end of section (a), and its consistency with the provisions of subsections (a)(2) and (a)(3) are other areas of concern. The amendment or elimination of these provisions may be appropriate.[74]

The ambiguities of these terms have apparently already created problems for federal law enforcement officials. For example, at a recent Congressional hearing, an assistant U.S. attorney in the District of Columbia indicated that he was having difficulty obtaining a grand jury indictment under the present Act, *inter alia*, because of the vagueness of the "use exemption."[75] An assistant U.S. attorney in Denver, Colorado, who obtained a conviction under the Act through a plea bargain, has expressed her concern regarding the imprecision of the Act's provisions, indicating that the law needs some refinements in order to withstand challenges that it is unconstitutionally vague.[76]

C. PENALTIES AND REMEDIES

The graduated penalties provided for in subsection (c) of the Act, including the felony/misdemeanor distinction, seem to be meritorious and appropriate. One could disagree with the level of the maximum

---

73. For example, S. 1678, *supra* note 2, contains definitions for the terms "computer," "computer system," "computer network," "computer program," "computer services," "financial institution," "financial instrument," "obtains access," "property," and "United States Government."

74. In addition, the official title of the Act, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, should be changed for the sake of clarity. The "counterfeit access device" provisions of the original version of the Act, H.R. 5112, were enacted separately and are codified at 18 U.S.C. § 1029 (Supp. II 1985). The "computer fraud" appellation is appropriate only if fraud provisions, similar to those of H.R. 1001 or H.R. 930, are added.

75. *Hearings*, *supra* note 48 (statement of David Geneson).

76. *See* Betts, *U.S. Attorneys Push to Clarify Vague '84 DP Crime Law*, COMPUTERWORLD, July 1, 1985, at 22.

fines and terms of imprisonment associated with the various offenses, but the attempt to have gradations in sanctions, according to the severity and the repetition of the offense, is reasonable.

Perhaps the most important consideration in reviewing the penalty provisions of the Act, or any other computer crime legislation, is the need to make civil remedies available to allow private litigants to recover losses resulting from violations of the Act. Given the narrow scope of the Act, any such civil remedies would also be of limited application. If the scope of the Act were broadened, such remedies would have greater significance.

Providing civil remedies in a criminal statute creates the prospect of increased litigation and the potential abuse of such remedies. The severe potential economic impact of computer crime on private parties, as well as the lack of other remedies and the scarcity of law enforcement resources, however, demonstrate the need for civil remedies and outweigh any potential negative consequences.

Several states have incorporated civil remedy provisions in their computer crime statutes. For example, Virginia's computer crime statute provides that "[a]ny person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained, and the costs of suit. Without limiting the generality of the term, 'damages' shall include loss of profits."[77] Congress should give similar language serious consideration.

None of the currently pending pieces of federal legislation includes civil remedy provisions. S. 1678, however, would add a forfeiture provision providing that:

> (d) Whoever violates any provision of paragraph (a), (b), or (c) shall forfeit to the United States any interest acquired or maintained in any computer and computer program, which has been used to commit the violation.[78]

Despite its laudable objective—deterring computer criminals by hitting them closest to home—this provision could create more administrative burdens and economic inefficiencies than it is worth in terms of deterrence. First, law enforcement officers have no existing mechanism in place to "dispose of all such property as soon as commercially feasible."[79] It is doubtful that the federal government would have any interest in keeping the diverse collection of computer equipment and programs that such confiscation schemes would net. Furthermore, it is likely that the federal government would incur expenses in developing a marketing or donation scheme for used computer equipment. Given

77. VA. CODE § 18.2-152.12A (Supp. 1985).

78. S. 1678, *supra* note 2.

79. *Id.*

the administrative costs of disposal and the fact that the computer equipment is worth the most to its experienced owner, it would appear that a confiscation system would be economically inefficient and unjustified. Moreover, for many of the teenage hackers from wealthy homes, confiscation would only result in the purchase of more up-to-date equipment. For those who are dependent on their computer for their livelihood, confiscation could impose undue hardship. In short, economic penalties for criminal offenders should be in the form of fines, not equipment confiscations.

D. INVESTIGATIVE AND PROSECUTORIAL JURISDICTION

The present Act raises two important jurisdictional issues. One is the effect of the Act on state and local jurisdiction over similar or identical offenses. The second concerns investigative jurisdiction at the federal level.

Concurrent federal/state and local jurisdiction over criminal offenses can be the source of problems, both in terms of the legal effect of federal criminal provisions on state and local law enforcement efforts and in terms of its practical effects on law enforcement at different levels. The effect of federal computer crime legislation on similar state legislation has been a subject of concern for some groups.[80]

The present Act does not address the issue of concurrent jurisdiction or the effect of the Act on state and local computer crime legislation. The major pending legislative proposals deal with concurrent jurisdiction, but in different ways.

H.R. 1001 and S. 1678 would both add the following provision:

> (f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.[81]

H.R. 930 would add the following provision:

> (3)(A) In a case in which Federal jurisdiction over an offense described in this subsection exists concurrently with State or local jurisdiction, the existence of Federal jurisdiction does not, in itself, require the exercise of Federal jurisdiction, nor does the initial exercise of Federal jurisdiction preclude its discontinuation.
>
> (B) In a case in which Federal jurisdiction over an offense described in this subsection exists or may exist concurrently with State or local ju-

---

80. *See, e.g.*, ABA TASK FORCE, *supra* note 3, app. II (resolution of the American Bar Association regarding federal computer crime legislation, approved by the ABA House of Delegates in Aug. 1979).

81. The predecessor of S. 1678, S. 2940, did not contain this or any other provision concerning concurrent jurisdiction.

risdiction, Federal law enforcement officers, in determining whether to exercise jurisdiction, should consider—

(i) the relative gravity of the Federal offense and the State or local offense;

(ii) the relative interest in Federal investigation or prosecution;

(iii) the resources available to the Federal authorities and the State or local authorities with respect to the offense;

(iv) the traditional role of the Federal authorities with respect to the offense;

(v) the interests of federalism; and

(vi) any other relevant factor.

(C) The Attorney General shall—

(i) consult periodically with representatives of State and local governments concerning the exercise of jurisdiction in cases in which Federal jurisdiction as described in this subsection exists or may exist concurrently with State or local jurisdiction;

(ii) report annually to the Congress concerning the extent of the exercise of such Federal jurisdiction during the preceding fiscal year; and

(iii) report to the Congress within one year after the date of the enactment of this Act on the long-term impact on Federal jurisdiction of this subsection and the increasingly pervasive and widespread use of the computers in the United States and periodically review and update such report.

(D) Except as otherwise prohibited by law, information or material obtained pursuant to the exercise of Federal jurisdiction over offenses described in this subsection may be made available to State or local law enforcement officers having concurrent jurisdiction over offenses arising from the same conduct and to State or local authorities otherwise assigned responsibility with regard to such conduct.

S. 440 contains similar language, but states that "Federal law enforcement officers . . . *shall* consider [the following factors]", instead of "should consider."[82] In addition, S. 440 provides that the Attorney General "*shall* provide general direction to Federal law enforcement officers concerning the appropriate exercise of such Federal jurisdiction which, for the purposes of investigation, is vested concurrently in the Department of Justice and the Department of the Treasury."

To the extent that federal "overreaching" is considered a serious potential problem, the paragraph contained in both H.R. 1001 and S. 1678 seems to be inadequate. The provisions of H.R. 930 and S. 440 go much farther toward ensuring federal restraint in federal computer crime cases. The use of "should consider" in H.R. 930 is preferable, however, to the "shall consider" mandate of S. 440. The "shall consider" clause would likely create unnecessary litigation concerning

82. S. 440, *supra* note 2 (emphasis added).

whether such factors were *in fact* considered by the relevant federal law enforcement officers, without any offsetting benefits. The other provisions of H.R. 930 and S. 440 (e.g., the requirements for consultation with state and local governments and an annual report concerning the exercise of federal jurisdiction) provide more than sufficient protection against federal overreaching.

The present Act places federal investigative jurisdiction with the U.S. Secret Service.[83] H.R. 5616 probably gave the Secret Service investigative jurisdiction over both the credit card fraud provisions[84] and the computer abuse provisions,[85] because the Secret Service has jurisdiction over many bank-related offenses. When Congress separated the computer abuse provisions from the credit card provisions, the investigative jurisdiction sections remained unchanged in both.

While Congress apparently did not give the matter of investigative jurisdiction serious deliberation prior to the passage of the present Act, it should do so now. It may be determined that it is entirely appropriate for the Secret Service to have investigative jurisdiction over the Act. Given the Act's coverage of intrusions into government computers and the acquisition of classified information, however, jurisdiction may more appropriately belong with the FBI. Other factors to be considered include the relative expertise of the Secret Service and the FBI in understanding computers and computer crime, and the willingness of each agency to devote resources to the enforcement of the Act.

The Act seems to contemplate concurrent investigative authority between the Secret Service and the FBI or "any other agency having such authority."[86] Having multiple agencies with investigative jurisdiction creates potential problems, which may or may not be solved by a memorandum of understanding between the agencies involved.

Regardless of where investigative authority is placed, the Act's requirement that the Attorney General report to Congress annually during the first three years following enactment on prosecutions under the Act will certainly aid Congressional oversight. Effective enforcement of the Act will require the commitment of resources and attention by the Department of Justice and other government agencies. To assist the Department of Justice and the Department of the Treasury in implementing the Act (if the Secret Service has investigative jurisdiction), Congress should consider the appropriation of funds specifically earmarked for the training of federal investigators and prosecutors in computer operations and computer crime. Federal law enforcement of-

83. 18 U.S.C. § 1030(d) (Supp. II 1985).

84. *Id.* § 1029.

85. *Id.* § 1030.

86. *Id.* § 1030(d).

ficials may never be able to stay ahead of computer hackers and committed computer criminals; but, the enactment of federal computer crime legislation will accomplish nothing if federal law enforcement officials are not given the training and the resources they need to keep abreast of the state of the art.

CONCLUSION

Congress is to be commended for enacting legislation making certain types of computer crime federal criminal offenses. The present Act, however, is very limited in scope and should be made more precise and consistent. After due deliberation, Congress should enact more cohesive and comprehensive computer crime legislation.

APPENDIX

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby obtains information contained in a financial record of a financial institution, as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(3) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;

shall be punished as provided in subsection (c) of this section. 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.

(b)(1) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

(c) The punishment for an offense under subsection (a) or (b)(1) of this section is—

(1)(A) a fine of not more than the greater of $10,000 or twice the value obtained by the offense or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine of not more than the greater of $100,000 or twice the value obtained by the offense or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(2)(A) a fine of not more than the greater of $5,000 or twice the value obtained or loss created by the offense or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2) or (a)(3) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine of not more than the greater of $10,000 or twice the value obtained or loss created by the offense or imprisonment for not [more] than ten years, or both, in the case of an offense under subsection (a)(2) or (a)(3) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section, the term "computer" means 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.