Western New England Law Review

Volume 7 7 (1984-1985)
Issue 3

Article 13

1-1-1985

CRIMINAL LAW—CONNECTICUT ADOPTS COMPREHENSIVE COMPUTER CRIME LEGISLATION: PUBLIC ACT 84-2061

William S. Allred

CRIMINAL LAW—CONNECTICUT ADOPTS COMPREHENSIVE COMPUTER CRIME LEGISLATION: PUBLIC ACT 84-206

I. INTRODUCTION

On May 31, 1984, Connecticut Governor William O'Neill signed into law a comprehensive computer crimes statute.[1] The successful passage of the legislation largely resulted from a growing awareness in the legislature of the vulnerability of computer systems to criminal manipulation and destruction.[2] The business and legal communities were instrumental in bringing the scope of the problem to the attention of state legislators.[3] This article will examine the Connecticut statute[4] and evaluate the extent to which the legislation is needed in its present form.[5]

II. THE STATUTE'S PROVISIONS

Generally, the act (1) establishes a definitional framework;[6] (2) delineates five separate computer crimes;[7] (3) prescribes penalties;[8] (4)

---

1. Act of May 31, 1984, Pub. Act No. 84-206, 1984 Conn. Legis. Serv. 193 (West). Connecticut's computer crime statute became effective on October 1, 1984. CONN. GEN. STAT. § 2-32 (1983)(effective date of public and special acts).

2. Experts estimate that computer crime losses in the United States alone range from $100 million to $10 billion annually. CHAMBER OF COMMERCE OF THE UNITED STATES, A HANDBOOK ON WHITE COLLAR CRIME: EVERYONE'S PROBLEM, EVERYONE'S LOSS 6 (1974); J. SOMA, COMPUTER TECHNOLOGY AND THE LAW, 264 (1983). *But see* Taber, *A Survey of Computer Crime Studies*, 2 COMPUTER/L. J. 275 (1980). Taber maintains that " 'computer crime' is insignificant." *Id.* at 310. He argues that the above cited figures are unverified and invalid and further that legislators have acted hastily in justifying a need for computer crime legislation on "inadequate research." *Id.* at 310-11.

3. *See infra* note 59 and accompanying text. For the past decade the problems associated with computer crimes have been the subject of increasing discourse among legislators, computer experts, and the bar throughout the United States. See D. PARKER, CRIME BY COMPUTER (1976), and Nycum, *The Criminal Law Aspects of Computer Abuse*, 5 RUTGERS J. COMPUTERS & L. 271 (1976) for early works by two of the most prominent experts in the field. *See also* A. BEQUAI, COMPUTER CRIME (1978). Their discourse drew widespread attention in Connecticut only within the past two years. *See infra* notes 54-60 and accompanying text.

4. *See infra* notes 6-53 and accompanying text.

5. *See infra* notes 54-93 and accompanying text. This article attempts to define as narrowly as possible the intent of the drafters of Connecticut's computer crime legislation.

6. Act of May 31, 1984, § 1, *supra* note 1, at 193-94. *See infra* notes 16-24 and accompanying text.

7. Act of May 31, 1984, § 2, *supra* note 1, at 194-95. *See infra* notes 25-37 and accompanying text.

authorizes civil actions;[9] and (5) addresses procedural matters that affect the application of the statute.[10]

Most of the drafters of Connecticut's statute assert that Public Act 84-206 represents a unique approach to computer crime legislation.[11] Generally, their claim is justified. A majority of the states that have adopted computer crime legislation[12] modeled their statutes after proposed federal legislation.[13] These versions have been widely criticized as being too broad and too harsh.[14] In both form and substance, however, the Connecticut statute parallels very closely a sister state's immediately preceding legislation—Delaware's computer crime statute.[15]

A. *Definitions*

The Connecticut computer crimes statute attempts to define the medium of the crime as well as the terms that the legislature expected

---

8. Act of May 31, 1984, §§ 3-9, *supra* note 1, at 195-96. *See infra* notes 38-44 and accompanying text.

9. Act of May 31, 1984, § 13, *supra* note 1, at 197-98. *See infra* notes 45-48 and accompanying text.

10. Act of May 31, 1984, §§ 10-12, 13(g), 13(h), *infra* note 1, at 196-98. *See infra* notes 49-53 and accompanying text.

11. Telephone interview with Linda O. Smiddy, Chairperson of the Ad Hoc Committee on Computer Crimes, Assoc. Partner of Cummings & Lockwood, Stamford, Conn. (Sept. 20, 1984). The drafters reviewed the legislation of at least 16 states that had already adopted computer crime legislation as well as proposed federal legislation before they began to frame the Connecticut draft. *Id.*

12. State statutes modeled after proposed federal legislation include: ARIZ. REV. STAT. ANN. § 13-2316 (1978); CAL. PENAL CODE § 502 (West Supp. 1985); COLO. REV. STAT. §§ 18-5.5-101 to -102 (Supp. 1984); FLA. STAT. ANN. §§ 815.01 to -.07 (West Supp. 1985); Act of Sept. 11, 1979, § 1, ILL. ANN. STAT. ch. 38, § 16-9 (Smith-Hurd Supp. 1984-1985); MICH. COMP. LAWS ANN. §§ 752.792 to -.797 (West Supp. 1984); N.M. STAT. ANN. §§ 30-16A-1 to -4 (1984); N.C. GEN. STAT. §§ 14-453 to -457 (1983); R.I. GEN. LAWS §§ 11-52-1 to -5 (1981 & Supp. 1984); UTAH CODE ANN. §§ 76-6-701 to -704 (Supp. 1983); VA. CODE § 18.2-152.1 to -.14 (Supp. 1984).

13. *See* S. 1766, 95th Cong., 2d Sess., 124 CONG. REC. 796 (1978); *Federal Computer Systems Protection Act: Hearings on S. 1766 Before the Subcomm. on Crim. Laws and Proc. of the Senate Comm. on the Judiciary*, 95th Cong., 2d Sess. (1978), *and* S. 240, 96th Cong., 1st Sess., 125 CONG. REC. 1190-91 (1979); *Computer Systems Protection Act of 1979: Hearings on S. 240 Before the Subcomm. on Crim. Just. of the Senate Comm. on the Judiciary*, 96th Cong., 2d Sess. (1980). Neither bill was enacted. *See also* Krieger, *Current and Proposed Computer Crime Legislation*, 2 COMPUTER/L. J. 721, 725-26 (1980)(reprints of proposed federal legislation).

14. Gemignani, *Computer Crime: The Law in '80*, 13 IND. L. REV. 681, 708-09 (1980); Taber, *On Computer Crime (Senate Bill S. 240)*, 1 COMPUTER L. J. 517, 523-37 (1979).

15. *Compare* Act of May 31, 1984, *supra* note 1 *with* DEL. CODE ANN. tit. 11, §§ 931-39 (Supp. 1984).

would arise in the ordinary course of prosecution under the statute.[16] The definitional section is the only portion of the statute that reveals strong positive influence by the provisions of other jurisdictions.[17] Negative influence is prominent as well. For instance, a number of jurisdictions that have considered computer crime legislation, including the federal government, have provided for definitional exclusions which limit the breadth of the legislation.[18] Drafters in Connecticut, as in a majority of states,[19] chose not to provide for limiting exclusions since further technological advances might make some exclusions obsolete.[20]

Assuming the drafters in Connecticut feared premature obsolescence, their definition of "computer" as an "electronic device"[21] is perplexing. Other state legislatures have exhibited greater consistency regarding the fear of obsolescence by including all known computer technologies in their definitions of "computer."[22] As one commentator noted, states that provide only for electronic devices may run into problems since "many computers of the future may not be electrical at all."[23] With computer technology advancing as rapidly as it has, amending Connecticut's definition of "computer" may become necessary sooner than anticipated.[24]

---

16. Act of May 31, 1984, § 1, *supra* note 1, at 193-94. Defining "computer crime" has not been easy. Even experts have failed to agree on a layman's definition for *computer*. The definition with which experts are in accord is lengthy and far too technical for legal use. Taber, *supra* note 14, at 532 n.88.

17. *Compare* Act of May 31, 1984, § 1, *supra* note 1, at 193-94 *with* S. 240, 96th Cong., 1st Sess., 125 CONG. REC. 1190-91 (1979)(The Computer Systems Protection Act of 1979 which was never enacted). *Compare* Act of May 31, 1984, § 1(2), *supra* note 1, at 193 *with* UTAH CODE ANN. § 76-6-702(2) (1983).

18. For example, the computer crime legislation in one state and proposed federal legislation explicitly exclude some personal and household computerized devices from the legislation's coverage. LA. REV. STAT. ANN. § 14.73.1-.5 (West Supp. 1985); Krieger, *supra* note 13, at 725-26 (discussing proposed federal legislation).

19. All states but Louisiana. *Compare* Louisiana statute *supra* note 18 *with* those listed at *infra* note 89.

20. Telephone interview with Linda O. Smiddy, *supra* note 11.

21. Act of May 31, 1984, § 1(a)(2), *supra* note 1, at 193.

22. For example, Pennsylvania's computer crime statute defines "computer" in part as "[a]n electronic, magnetic, optical, hydraulic, organic *or other* high speed data processing device or system . . . ." 18 PA. CONS. STAT. ANN. § 3933(c) (Purdon Supp. 1984-1985)(emphasis added). *See also* N.C. GEN. STAT. §§ 14-453(2) (1981)("an internally programmed, automatic device").

23. Gemignani, *supra* note 14, at 681 n.3.

24. The chairperson of the ad hoc committee, Linda O. Smiddy, contends that even a state such as Pennsylvania will eventually run into problems since drafters cannot possibly foresee every technological advance. Telephone interview with Linda O. Smiddy, *supra* note 11. The fact is, however, that some of the forms of computers listed in the Pennsylvania statute, 18 PA CONS. STAT. ANN. § 3933(c) (Purdon Supp. 1984-1985) are existing

B. *Crimes*

The Connecticut statute establishes five categories of computer crimes: (1) unauthorized access; (2) theft of computer services; (3) disruption of computer services; (4) misuse of computer system information; and (5) destruction of computer equipment.[25] The legislature intended the five criminal provisions to be interpreted liberally.[26] Moreover, the provisions indicate that a *computer system* and not merely a *computer* is the object of the crime.[27] The distinction is significant since "computer system" includes more definitionally than "computer."[28]

In the process of proscribing certain computer-related activities, the drafters meant to create categories or levels of crime rather than specific crimes defined by example.[29] Arguably, an operative premise to the crimes section can be inferred from the statute's history and wording. The premise presupposes that all computer crime in its purest conceptual form represents an intentional disregard of a given scope of authorization.[30] One is not guilty of computer crime, that is,

---

or emerging technologies, *See Federal Computer Systems Protection Act: Hearings on S. 1766 Before the Subcomm. on Crim. Laws and Proc. of the Senate Comm. on the Judiciary*, 95th Cong., 2d Sess. 67 (1978) (testimony of D. Parker), and today's legislators must address them. Moreover, Pennsylvania's statute contains a catch all phrase ("or other") to obviate the potential need for future amendment. 18 PA. CONS. STAT. ANN. § 3933(c). *But cf.* Interim Proceedings of the Joint Committee on the Judiciary of the State of Connecticut 473 (Dec. 5, 1983) (remarks demonstrating an awareness of rapid technological advancement and a desire to draft a bill reflecting that understanding) [*hereinafter cited as* Interim Proceedings].

25. Act of May 31, 1984, § 2, *supra* note 1, at 194-95. A sixth but conceptually different crime exists in the event that one "recklessly engages in conduct which creates a risk of serious physical injury to another person" during the execution of any of the five enumerated categories of crime. *Id.* § 5(a)(2), *supra* note 1, at 195.

26. Telephone interview with Howard T. Owens, Jr., Conn. state senator since 1975, Co-chairman of the Joint Committee on the Judiciary, and senior partner of Owens & Schine, Bridgeport, Conn. (Sept. 25, 1984). *See also*, Interim Proceedings, *supra* note 24, at 467,477 (chairperson Smiddy's views as to how the committee dealt with the elusive nature of computer crimes).

27. Act of May 31, 1984, § 2, *supra* note 1, at 194-95.

28. " 'Computer system' means a computer, its software, related equipment, communications facilities, if any, and includes computer networks." *Id.* § 1(a)(7), *supra* note 1, at 193-94.

29. Telephone interview with Linda O. Smiddy, *supra* note 11. *See also*, Interim Proceedings, *supra* note 24, at 470-71 (remarks of Mr. Post suggesting criminal categories of computer crime).

30. One commentator defines computer crime as "the use of the computer or its technology as a target of or a tool for illegal purposes." SOMA, *supra* note 2, at 265. While the functional distinction among computer crimes in Connecticut rests on scope of authorization, *see* Act of May 31, 1984, § 2, *supra* note 1, at 194-95, the legislature apparently intended that one would not be "authorized" to do an illegal act.

one does not meet the threshhold of a criminal category, without first exceeding the bounds of his authorization.[31] Thus, each level of crime, from section 2(a) to 2(f), contemplates the existence of broader and broader user authority.[32] This is a rational scheme for delineating among categories of computer crime as it is readily comprehendible to the layman.

Unfortunately, the statutory wording in section two is ambiguous.[33] The first crime, unauthorized access,[34] definitely requires scienter;[35] that is, individuals must have known or reasonably should have known that they had no authorization to access a computer. The statute expressly provides the accused with an affirmative defense: if he/she can show a lack of scienter, he/she will avoid conviction.[36] In the remaining crimes, however, the requirement of scienter is arguably unclear.[37]

The second crime, for instance, requires an "intent to obtain unauthorized computer services."[38] The lack of an express affirmative defense for those accused of the second crime, or any of the remaining crimes for that matter, makes the requirement of scienter questionable. What if the defendant accessed and obtained a service believing he/she had authorization to do so when, in fact, he/she did not? Did the drafters mean for intent to be read into the word "unauthorized"? If so, then a conviction in the hypothetical should fail for a lack of intent. If, however, the word "unauthorized" is not an aspect of intent but merely modifies "computer services," then the conviction would succeed since the defendant's knowledge of the service's status would be irrelevant. As long as he/she accessed the service—whether he/she knew he/she was allowed to or not—and it was his/her purpose to do so, the criminal elements will have been established.

---

31. *See* L. Smiddy & J. Smiddy, *Connecticut's New Computer Crime Law*, Conn. L. Tribune, Nov. 19, 1984, at 1, 6, col.2 (passage implying the scope of authorization premise). For example, an individual may be authorized to access a computer while unauthorized to access certain services provided by the system. An individual with greater authority may be authorized to use all of a system's services and programs, but not to alter data or remove computer equipment. The widest scope of authority applies to those individuals with maintenance authority of the computer system such that they may delete data or, perhaps, remove equipment from the system. *Id.*

32. *See* Act of May 31, 1984, §§ 2(a)-(f), *supra* note 1, at 194-95.

33. *Id.* § 2, *supra* note 1, at 194-95.

34. *Id.* § 2(b)(1), *supra* note 1, at 194.

35. Defined herein as *guilty knowledge*. BLACK'S LAW DICTIONARY 1207 (rev. 5th ed. 1979).

36. Act of May 31, 1984, § 2(b), *supra* note 1, at 194.

37. *Id.* §§ 2(c)-(f), *supra* note 1, at 194-95.

38. *Id.* § 2(c), *supra* note 1, at 194.

The crucial issue not clearly addressed by the drafters, therefore, is a distinction between wrongful intent and a mere intent to act, scienter not being an inherent element of the latter.[39]

C. *Penalties*

The drafters largely patterned the penalties provisions after Connecticut's larceny statute.[40] For the purpose of penalization, six criminal classifications exist within the larceny statute: three orders of felonies and three orders of misdemeanors.[41] The computer crime statute has been subdivided into similar classifications delineated by similar criteria.[42] The value of the damage or of the misappropriated service determines the gravity of the crime.[43] Punishment is by fine or imprisonment or both.[44] For valuation, the statute stipulates that

---

39. As Justice Oliver Wendell Holmes once wrote, "[a]n act is always a voluntary muscular contraction, and nothing else. The chain of physical sequences which it sets in motion or directs to the plaintiff's harm is no part of it." O. W. HOLMES, THE COMMON LAW 91 (1938). Moreover, the United States Supreme Court has held that one cannot presume a wrongful intent from an act itself. Morissette v. United States, 342 U.S. 246 (1952). In *Morissette*, the defendant had taken metal bombshell casings from government land thinking that since they had been there for four years they had been abandoned. The government brought an action for criminal conversion, and the court noted:

> That the removal of [the casings] was a conscious and intentional act was admitted. But that isolated fact is not an adequate basis on which the jury should find the criminal intent to steal or knowingly convert, that is, *wrongfully* to deprive another of possession of property.

Id. at 276. Thus, in the hypothetical mentioned in the text, it would not be fair to presume criminal intent from the accused's use of a service later learned to be unauthorized.

40. Telephone interview with Linda O. Smiddy, *supra* note 11. *Compare* Act of May 31, 1984, §§ 3-7, *supra* note 1, at 195-96 *with* CONN. GEN. STAT. §§ 53a-122 to -125(b) (1983).

41. CONN. GEN. STAT. §§ 53a-122 to -125(b) (1983).

42. Only five classes of computer crime exist: computer crimes in the first to the fifth degree correspond to similar classes of crime as provided in the larceny statute, *see* CONN. GEN. STAT. §§ 53a-122 to -125(b) (1983).

43.

COMPUTER CRIME	CRIME CLASS	VALUATION OF DAMAGE (determines criminal class)
1st Degree	Class B Felony	exceeds $10,000
2nd Degree	Class C Felony	exceeds $ 5,000
3rd Degree	Class D Felony	exceeds $ 1,000
4th Degree	Class A Misdemeanor	exceeds $ 500
5th Degree	Class B Misdemeanor	$500 or less

Act of May 31, 1984, §§ 3-7, *supra* note 1, at 195-96.

44. Corresponding penalties for each criminal class are as follows:

market value at the time of the violation shall be the measuring stick.[45] When market values are not ascertainable the statute provides gap-filler valuations.[46]

D. *Civil Actions and Other Provisions*

The Connecticut statute is one of only two state statutes to expressly allow civil actions arising out of computer crimes.[47] Moreover, the statute authorizes any "aggrieved person" who has reason to suspect that someone has engaged, is engaging, or will engage in a computer crime to file a lawsuit against the suspected offender.[48] In addition to seeking actual damages,[49] the aggrieved person may also seek (1) an injunction to restrain the accused from engaging in the act;

COMPUTER CRIME	IMPRISONMENT (discretionary)	FINES (discretionary)
Class B Felony	1 to 20 years	not to exceed $10,000
Class C Felony	1 to 10 years	not to exceed $5,000
Class D Felony	1 to 5 years	not to exceed $5,000
Class A Misdemeanor	up to 1 year	not to exceed $1,000
Class B Misdemeanor	up to 6 months	not to exceed $1,000

CONN. GEN. STAT. §§ 53a-35(a), 53a-35(b), 53a-36(1), 53a-36(2), 53a-41, 53a-42 (1983).

If persons gain money, property, services, or other items of value as a result of their activities, however, the court may fine them up to twice the amount of their aggregate gain instead of imposing the statutorily mandated fine *and* order incarceration. *Id.* § 53a-44. The decision rests within the judge's discretion. Act of May 31, 1984, § 8, *supra* note 1, at 196.

Where individuals have been found guilty of more than one section 2 violation, moreover, the damages assessed against them for each violation may be aggregated to determine the classification of their crimes. *Id.* § 9, *supra* note 1, at 196. For example, if an individual illegally procures and sells a program worth $900 in one instance and then illegally destroys a $4,500 terminal in another, a conviction of computer crime in the second degree may follow since the assessed damages of each violation aggregate to an amount exceeding $5,000. If the amounts of each violation were not aggregated, he/she would be guilty of computer crimes in the fourth and third degrees, respectively.

45. Act of May 31, 1984, § 10(a), *supra* note 1, at 196.

46. *Id.* §§ 10(b), 10(c), *supra* note 1, at 196.

47. *Id.* § 13, *supra* note 1, at 197-98. Only Delaware, DEL. CODE ANN. tit. 11, §§ 931-39 (Supp. 1984), and Connecticut have passed comprehensive computer crime legislation that expressly authorizes the filing of civil actions. The Illinois and South Dakota statutes merely provide that computer crime legislation does not affect rights to civil action. ILL. ANN. STAT. ch. 38, § 16-9(d) (Smith-Hurd Supp. 1984-1985); S.D. CODIFIED LAWS ANN. § 43-43B-7 (1983). In Connecticut, moreover, criminal prosecution is not a prerequisite to the filing of a civil action. Act of May 31, 1984, § 13(f), *supra* note 1, at 198.

48. Act of May 31, 1984, § 13(a), *supra* note 1, at 197-98.

49. A person who suffers injury to person, property, or business may sue to recover actual damages which may include nonpecuniary damages such as emotional distress. Where malicious or wilful conduct can be shown, the injured party may recover treble damages. Moreover, the prevailing plaintiff will recover costs and attorney's fees. *Id.* § 13(c)-13(e).

(2) an order directing restitution; or (3) an order directing the appointment of a receiver.[50]

Other provisions within the statute are also unique. For example, it waives sovereign immunity.[51] The impetus for the statute's significant waiver arose from the legislators' concern of protecting privacy.[52] The statute also provides for a broad grant of jurisdiction to Connecticut courts,[53] judicial authority to determine proper venue,[54] and a three-year statute of limitations.[55]

III. THE NEED FOR COMPREHENSIVE LEGISLATION

A. *Background*

Legislators had first attempted to bring computer crime legislation to Connecticut in 1980. In that year the Joint Committee of the Judiciary introduced a house bill containing comprehensive computer crime legislation.[56] Richard Tulisano, one of the sponsors of the bill, admits that the Committee introduced the measure to educate Connecticut legislators about the existence of a real and potentially threatening problem.[57] Yet, the bill had no foundation of interest or awareness in Connecticut. Few interest groups, if any, had lobbied for such legislation.[58] As a result, most legislators treated the bill with

---

50. *Id.* §§ 13(a)(1) to 13(a)(3), *supra* note 1, at 197-98.

51. *Id.* § 13(g), *supra* note 1, at 198. An amendment to the original house bill, H.B. 5041, 1984 Sess., included the waiver of sovereign immunity. "The substance of [the] amendment was originally intended to be included in the bill, but was not through some oversight." Conn. H. R. Proc., p. 1998 (April 18, 1984).

52. Telephone interview with Richard F. Tulisano, Conn. state representative and Co-chairman of the Joint Committee of the Judiciary, Hartford, Conn. (Sept. 28, 1984). The act protects private personal data from any unauthorized intrusion by either a private individual or the government.

> Private personal data is data concerning a natural person which a reasonable person would want to keep private and which is protectable under law. Not all information about an individual is automatically protected. There must be some common law or statutory basis for protection other than [this act].

Smiddy and Smiddy, *supra* note 31, at 6, col. 3. For concerns relating to the protection of private information stored in computer systems, see Comment, *The Use and Abuse of Computerized Information: Striking a Balance Between Personal Privacy Interests and Organizational Information Needs*, 44 ALB. L. REV. 589 (1980).

53. Act of May 31, 1984, § 11, *supra* note 1, at 197.

54. *Id.* § 12, *supra* note 1, at 197.

55. *Id.* § 13(h), *supra* note 1, at 198. The statute of limitations begins to run at the time the alleged violation is or should have been discovered. *Id.*

56. H.B. 6034, 1980 Sess., Conn. (introduced on March 20, 1980).

57. Telephone interview with Richard F. Tulisano, *supra* note 52.

58. *Id.* Connecticut only slowly became aware of the problem for a number of reasons. Evidence later revealed in committee hearings shows that the business community had been aware of the computer abuse problem for quite some time but had never been

indifference and suspected it dealt with an insignificant problem. Not surprisingly, the bill died in committee.[59]

A subsequent increase in the number of complaints from business and industry concerning several forms of computer fraud and abuse signaled a growth of awareness of computer crime in Connecticut.[60] Once aware of and threatened by the problem, business, legal, and government interests began lobbying for legislative protection.[61] By September, 1983, former state senator Russell Post had formed an ad hoc committee[62] to research computer crime in Connecticut and, further, to draft legislation to meet the problem.[63]

B. *The Inadequacy of Existing Law*

The ad hoc committee looked to existing criminal law first to determine whether Connecticut needed additional legislation. The ad hoc committee and many legislators reached a consensus that existing Connecticut law inadequately provided for the prosecution of many computer crimes.[64]

---

vocal about it. Interim Proceedings, *supra* note 24, at 456; SOMA, *supra* note 2, at 269. For much of the business community, the problem is a sensitive one since breaches of a firm's computer security system reflect on that firm's integrity. Reporting the breaches would create an image of instability. *Id.* at 269-70; Volgyes, *The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review*, 2 COMPUTER/L. J. 385, 394 (1980).

59. Telephone interview with Richard F. Tulisano, *supra* note 52. The technological complexity of the issues involved tends to intimidate lawmakers as well as members of the judiciary, many of whom have no formal education in computer technology. Gemignani, *supra* note 14, at 686.

60. Telephone interview with Richard F. Tulisano, *supra* note 52. For several years, the Connecticut Business and Industry Association (CBIA) received several state-wide reports decsribing instances of theft and interruption of services; destruction of computer equipment; destruction or alteration of software; unauthorized access; embezzlement; fraud; and disclosure of confidential information. Interim Proceedings, *supra* note 24, at 456-57. Experts note that the number of computer crimes has been increasing. Each instance of computer crime results, on the average, in a $450,000 loss, D. PARKER, FIGHTING COMPUTER CRIME 25 (1983), a significant loss for even the largest corporation.

61. Telephone interview with Richard F. Tulisano, *supra* note 52. *See also* Interim Proceedings, *supra* note 24, at 453-54.

62. Telephone interview with Howard T. Owens, *supra* note 26; Interim Proceedings, *supra* note 24, at 455-57. Representation on the ad hoc committee included the business and the financial communities (New England Telephone, Phoenix Mutual Life Insurance Company, General Electric, Perkin-Elmer, IBM, Connecticut Bank & Trust, United Technologies, and the CBIA) and the legal and governmental communities (Cummings & Lockwood, the Chief State's Attorney of Connecticut, and former U.S. Attorney Richard Blumenthal). *Id.* at 453-54.

63. Telephone interview with Howard T. Owens, *supra* note 26.

64. Telephone interview with Linda O. Smiddy, *supra* note 11. *See also* N.Y. Times, Sept 18, 1983, at A1, col. 1. *But see* SOMA, *supra* note 2, at 263 n.8 (views of John Taber

Before computer crime legislation existed, governments prosecuted computer crimes under traditional common law or statutory crimes, such as larceny,[65] theft of services,[66] and theft of trade secrets.[67] One commentator suggested the use of other established criminal provisions including credit card fraud, burglary, telephone abuse, and criminal mischief.[68] Since most of these crimes[69] evolved long before the advent of the computer, they fail to take into account novel forms of property and other characteristics peculiar to computer crime.[70] In some states, for example, property subject to larceny must be a tangible article.[71] Moreover, the taking or asportation[72] of the article must permanently or significantly deprive the owner of the use of the object.[73]

In *Lund v. Commonwealth*,[74] for instance, a graduate student gained the use of a school computer system by fraudulently entering the access numbers of other registered users. He used more than $26,000 worth of unauthorized computer time.[75] The jury found the student guilty of grand larceny. On appeal, the Virginia Supreme Court reversed the conviction holding that the theft of computer time

---

that existing criminal law is adequate); Comment, *Legislative Issues in Computer Crime*, 21 HARV. J. ON LEGIS. 239, 241-42 (1984)(existing criminal law adequate).

65. Lund v. Commonwealth, 217 Va. 688, 232 S.E.2d 745 (1977).

66. State v McGraw, 459 N.E.2d 61 (Ind. App., 2d Dist. 1984).

67. Ward v. Superior Court of California, 3 Computer L. Serv. Rep. (Callaghan) 206 (Cal Super. Ct. 1972)(mem.).

68. Nycum, *supra* note 3, at 285-93.

69. A key controversy in the debate on the structure of computer crime legislation concerns whether crimes by computer involve traditional crimes perpetrated by new means, or whether they are entirely new forms of crime. "The preponderance of opinion . . . supports the view that the computer has changed both the form and means by which the traditional crimes . . . are created." Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMPUTER L. J. 353, 362 (1980).

70. Smiddy & Smiddy, *supra* note 31, at 1, col.1. Connecticut statutes on point include CONN. GEN. STAT. § 53a-119(7) (1983)(theft of services); *id.* § 31-40n (1983)(theft of trade secrets applying only to information concerning toxic substances); *id.* §§ 53a-128a to -128i (1983)(credit card crimes); *id.* §§ 53a-100 to -104 (1983)(burglary applying only where a building is physically entered); *id.* §§ 53a-187 to -188 (1983)(telephone abuse); *id.* §§ 53a-115 to -117 (1983)(criminal mischief applying only to a tampering with tangible property).

71. CONN. GEN. STAT. § 53a-118 (1983); HAWAII REV. STAT. § 708-800(15) (1976); N.Y. PENAL LAW § 155.00(1) (McKinney Supp. 1984-1985).

72. *See infra* note 84.

73. *See* CONN. GEN. STAT. § 53a-119 (1983); *see also* SOMA, *supra* note 2, at 274-75 (discussion of the significance of asportation in Ward v. Superior Court of California, 3 Computer L. Serv. Rep. (Callaghan) 206 (Cal. Super. Ct. 1972)).

74. 217 Va. 688, 232 S.E.2d 745 (1977).

75. *Id.* at 690, 232 S.E.2d at 747.

did not constitute larceny under the Virginia Code.[76] Other statutes would almost certainly fail because of similar limitations.[77]

Conversely, courts in some states have interpreted existing statutes broadly so as to include computer crimes.[78] Yet, little uniformity can be expected when the application of a statute turns on the philosophy of an individual.[79] Only new legislation can remedy the various inadequacies of traditonal laws.

C. *Alternatives*

1. Redefining the Law

Some commentators intimate that many of the problems associated with the prosecution of computer crime under traditional laws could be solved by legislatively expanding traditional criminal concepts.[80] The approach calls for the redefinition of terms such as "property" and "theft of services" so as to encompass crimes committed with the aid of computers.[81] Still, in some states where older concepts have been expanded,[82] whether the "new" statutes will be

---

76. *Id.* at 691-92, 232 S.E.2d at 748. Maryland and Florida used a tangibility test similar to the one employed by Virginia courts with respect to property in larceny statutes. *Federal Computer Systems Protection Act of 1976: Hearings on S. 1766 Before the Senate Comm. on the Judiciary*, 95th Cong., 2d Sess. (1979). Delaware and New Jersey also used a tangibility test. Nycum, *supra* note 3, at 281, 284. *See also* Comment, *Computer Crime—Senate Bill S. 240*, 10 MEM. ST. U. L. REV. 660, 663-64 (1980).

77. Connecticut's burglary statute, for example, requires an entering of the premises. *See* CONN. GEN. STAT. § 53a-101 (1983).

78. *See, e.g.*, State v. McGraw, 459 N.E.2d 61 (Ind. App., 2d Dist. 1984); *see also* U.S. v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979)(describing unauthorized computer usage as a trespass upon physical property).

79. As a result of the subjectivity inherent in the "intrinsic values" of ideas, judges may act out of moral or political convictions. *See* P. SAYRE, PHILOSOPHY OF LAW 10-12 (1981). Moreover, while precedent binds judges, they are "under no obligation to follow any particular precedent." L. CARTER, REASON IN LAW 32 (1979). Judges exploit what Dr. Lief Carter, an eminent commentator, calls "fact freedom" to decide which facts in the case before them are material thereby making their choice of which precedent to follow somewhat discretionary. *Id.* Conceivably, possibly inevitably, judges will be guided by their own moral or political philosophy in making their choices. Two factually similar cases, therefore, though governed by the same statute, may well have inconsistent outcomes where the judges espouse different personal philosophies.

80. Comment, *supra* note 64, at 241-42; *see id.* at 254 (traditional concepts obselete).

81. *See, e.g.* ALA. CODE § 13A-8-1(10) (1982)(defining property as "[a]ny money, [or] tangible or intangible personal property"); TEX. PENAL CODE ANN. § 31.01(6)(B) (Vernon Supp. 1984)(property means "tangible or intangible personal property . . ."); § 31.01(7)(B) (for purposes of theft of services any telecommunication is subject to theft).

82. *See, e.g.* ALA. CODE § 13A-8-1(10) (1982); FLA. STAT. ANN. § 812.012 (West Supp. 1984); GA. CODE § 16-1-3(13) (1984); IND. CODE ANN. § 35-41-1-23 (West Supp. 1984-1985); IOWA CODE ANN. § 702-14 (West 1979); ME. REV. STAT. ANN. tit. 17A, § 352 (1983); MD. ANN. CODE art. 27, § 340(h) (1982); MASS. GEN. LAWS ANN. ch. 266,

sufficient for prosecution of computer crimes has not yet been established.[83] More specifically, the Connecticut ad hoc committee confronted as a major concern whether simply redefining the law would criminalize such activities as unauthorized access of a computer and computer services, especially when the wrongdoer memorizes rather than copies the accessed data.[84] Although some states have redefined their theft of services statutes,[85] even they might not cover the unauthorized access of computers.[86]

2. Comprehensive Computer Crime Legislation

While the redefinition of certain crimes would be sufficient for the prosecution of the more serious computer crimes, at least two undesirable effects would result. First, the less serious computer crimes would still elude prosecution.[87] Second, redefining traditional law would create entirely new and serious problems in prosecuting the

---

§ 30(2) (West 1983); NEB. REV. STAT. § 28-509(5) (1979); N.J. STAT. ANN. § 2C:20-1(g) (West 1982); OHIO REV. CODE ANN. § 2901.01(J)(1) (Page Supp. 1983); TEX. PENAL CODE ANN. § 31.01(6) (B) (Vernon Supp. 1984).

83. *See* Nycom, *supra* note 3, at 284.

84. Telephone interview with Linda O. Smiddy, *supra* note 11. Common law larceny requires asportation, or the phsyical action of carrying away the object of the theft. W. LAFAVE & A. SCOTT, HANDBOOK ON CRIMINAL LAW 631-33 (1972). Recent redefinitions of statutory concepts, such as California's trade secret law, continue to require asportation. CAL. PENAL CODE § 499c (West 1983). In Ward v. Superior Court of California, the defendant walked away with, or asported, a printed paper copy—a physical object. Ward v. Superior Court of California, 3 COMPUTER L. SERV. REP. (Callaghan) 206 (Cal. Super. Ct. 1972). What if instead of copying the data he had memorized it and walked away? Clearly, he would not have been guilty of theft since no asportation would have occurred. *Id.* at 210. He would have merely engaged in the unauthorized access of a computer. California legislators amended § 499c, effective January 1, 1984, to address the problem. Currently under § 499c, a "person is guilty of theft who . . . steals, takes, carries away, *or uses without authorization* a trade secret." CAL. PENAL CODE § 499c(b)(1) (West Supp. 1983-1984). Massachusetts and Pennsylvania have eliminated the requirement of asportation in their trade secret statutes, although Massachusetts still requires a copying. Nycum, *supra* note 3, at 283. The Connecticut statute also eliminates the element of asportation. Act of May 31, 1984, § 2(e), *supra* note 1, at 194-95. Many states' computer crime laws "require the information to be a trade secret [before it will be protected by statute]. Connecticut's law, however, will protect all information stored on a computer whether it is a trade secret or not." Smiddy and Smiddy, *supra* note 31, at 6, col.3.

85. IND. CODE ANN. § 35-43-4-2 (West Supp. 1984-1985); ME. REV. STAT. ANN. tit. 17A, § 357 (1964); MD. ANN. CODE art. 27, § 340 (j) (1982); N.H. REV. STAT. ANN. § 637:8 (1974 & Supp. 1983); OHIO REV. CODE ANN. §§ 2913.01 to - .02 (Page Supp. 1983).

86. A computer system can serve only a specified number of users at a given time. The system cannot be accessed when its services are fully committed. An unauthorized access, therefore, even though not beyond the services menu, will prohibit an authorized user from gaining access when the system is working to capacity.

87. *See supra* notes 82-83 and accompanying text.

traditional crimes. For example, a new definition of larceny that lacked the common law element of asportation would be anathema to the underlying concept of larceny.[88]

In order to address potential uncertainty regarding the scope of statutes that merely redefine and to avoid disturbing a criminal system that deals fairly well with the more traditional problems, many legislators chose the option of establishing a separate body of computer crimes.[89] They thus obviated the need to restructure substantially a traditional and familiar body of criminal law and also focused legislative attention on issues related to computer abuse. The greater legislative specificity, in turn, yields greater structural stability through more predictable judicial interpretation.[90]

In addition, with comprehensive statutes, legislators can focus on concerns other than defining the crimes. For instance, although a statute providing for fines and incarceration would punish the wrongdoer, it would not make the injured party whole. The committee members, accordingly, authorized civil actions so that the injured party could obtain redress.[91] In those cases where defendants are not judgment-proof, victims will be able to recover their losses.[92]

In short, the drafters of Connecticut's computer crime statute sought to do more than provide legislative clarity. Other concerns in-

---

88. *See supra* note 81.

89. Twenty eight states and the District of Columbia have adopted comprehensive computer crime legislation: ALASKA STAT. §§ 11.46.200, .484, .740, .985, .990 (1983); ARIZ. REV. STAT. ANN. § 13-2316 (1978); CAL. PENAL CODE § 502 (West Supp. 1985); COLO. REV. STAT. §§ 18-5.5-101 to -102 (Supp. 1984); Act of May 31, 1984, Pub. Act No. 84-206, 1984 Conn. Legis. Serv. 193 (West); DEL. CODE ANN. tit. 11, §§ 931-39 (Supp. 1984);D.C. CODE ANN. §§ 22-3801, -3811, -3821, -3823 (Supp. 1984); FLA. STAT. ANN. §§ 815.01-.07 (West Supp. 1985); GA. CODE §§ 16-9-90 to -95 (1984); IDAHO CODE §§ 18-2201 to -2202 (1984); ILL. ANN. STAT. ch. 38, § 16-9 (Smith-Hurd Supp. 1984-1985); KY. REV. STAT. ANN. §§ 484.840, .845, .850, .855 (Bobbs-Merrill Supp. 1984); LA. REV. STAT. ANN. § 14.73.1 to -.5 (West Supp. 1985); MICH. COMP. LAWS ANN. §§ 752.791 to -.797 (West Supp. 1984); MINN. STAT. ANN. §§ 609.87 to -.89 (West Supp. 1984); MO. ANN. STAT. §§ 569.093 to -.099 (Vernon 1985); MONT. CODE ANN. §§ 45-2-101, -6-310 to -311 (1983); N.M. STAT. ANN. §§ 30-16A-1 to -4 (Supp. 1984-1985); N.C. GEN. STAT. §§ 14-453 to -457 (1983); N.D. CENT. CODE §§ 12.1-06.1-01, 12.106.1-08. (Supp. 1983); OKLA. STAT. ANN. tit. 21, §§ 1951-56 (West Supp. 1984-1985); PA. CONS. STAT. ANN. § 3933 (Purdon Supp. 1984-1985); R.I. GEN. LAWS §§ 11-52-2 to -5 (1983); S.D. CODIFIED LAWS ANN. § 43-43B (Supp. 1984); TENN. CODE ANN. §§ 39-3-1401 to -1406 (Supp. 1984); UTAH CODE ANN. §§ 76-6-701 to -704 (Supp. 1983); VA. CODE § 18.2-152.1 to -152.14 (Supp. 1984); WIS. STAT. ANN. § 943.70 (West Supp. 1984-1985); WYO. STAT. §§ 6-3-501 to -505 (1983).

90. The need for a liberal and more effective judicial and criminal system compels the adoption of comprehensive legislation. Comment, *supra* note 64, at 240-41.

91. Telephone interview with Linda O. Smiddy, *supra* note 11.

92. *See* Act of May 31, 1984, §§ 13(b), 13(c), *supra* note 1, at 198.

cluded protection of privacy,[93] compensation to the injured party,[94] provision for a clear deterrent to a potential wrongdoer,[95] and the elimination of sovereign immunity.[96] The drafters found comprehensive computer crime legislation necessary in order to address all of their concerns simultaneously.

D. *Potential Problems*

The greatest single problem inherent in any criminal legislation results from the fact that the crime must be detected and reported before it can be prosecuted.[97] Presently, experts estimate that only 1 to 15 out of every 100 computer crimes are reported.[98] The root of the problem lies in the sophistication of computer technology which allows wrongdoers to erase every trace of their acts within the very algorithm they use to perpetrate the crime.[99] While at least one state has made reporting computer crimes a legal duty,[100] the legislature can do little to overcome this very significant problem.

Moreover, once the crime is reported, attempts to prosecute may be stymied by evidentiary problems. In order to prove the criminal elements beyond a reasonable doubt, the prosecution must rely on evidence. Yet, current rules of evidence[101] are arguably inadequate for the prosecution of a computer crime.[102] The basic issue involves whether computer-generated evidence such as a paper printout, reel or disk recording, or punched data card will be admissible as an excep-

---

93. Telephone interview with Richard F. Tulisano, *supra* note 52.

94. *See supra* notes 47-50 and accompanying text.

95. Telephone interview with Richard F. Tulisano, *supra* note 52.

96. *See supra* note 51 and accompanying text.

97. Note, *A Suggested Legislative Approach to the Problem of Computer Crime*, 38 WASH. & LEE L. REV. 1173, 1179-80 (1981).

98. A. BEQUAI, COMPUTER CRIME: A TWENTIETH CENTURY CRISIS xiii (1978).

99. Interim Proceedings, *supra* note 24, at 477. Known as 'burying a time bomb,' the technique completely prevents detection. *See* Smiddy and Smiddy, *supra* note 31, at 6, col.2.

100. GA. CODE § 16-9-95 (1984).

101. *See, e.g.*, CONN. GEN. STAT. § 52-180 (1983). For a comparison of the Federal Rules of Evidence with the Connecticut Law of Evidence, see Tait, *The New Federal Rules of Evidence: A Summary of Differences Between the Rules and Connecticut Law of Evidence*, 9 CONN. L. REV. 1 (1976).

102. *See generally* Johnston, *A Guide for the Proponent and Opponent of Computer Based Evidence*, 1 COMPUTER/L. J. 667 (1979)(reviews methods for overcoming obsolete evidence rules, including the grounds upon which to prevent or to allow evidence into admission); Singer, *Proposed Changes to the Federal Rules of Evidence as Applied to Computer-Generated Evidence*, 7 RUTGERS J. COMPUTERS & L. 157 (1979)(inadequacy of Federal Rules of Evidence due largely to the lack of a fundamental understanding of electronic data processing on the part of individuals of the legal community).

tion to both the hearsay and best evidence rules.[103] Getting computer-generated evidence admitted can still be difficult under existing evidence rules.[104]

IV. CONCLUSION

While businesses may have been reluctant to publicize the breach of their computer systems in the past,[105] the increase in the number of computer crimes has forced businesses to publicly acknowledge the problem and call for protective legislation in order to avoid absorbing computer crime related losses.[106] Pressure from business as well as legal and governmental circles culminated in the convocation of the ad hoc committee in Connecticut.[107]

After examining whether state and federal laws were adequate for the prosecution of computer crimes, or more generally, for the protection of the business community, the ad hoc committee concluded that new legislation was needed.[108] Moreover, several other states, having already studied the problem within their own jurisdictions, came to the same conclusion and adopted computer crime legislation.[109] Some had chosen merely to redefine traditional legal concepts,[110] while others had chosen to enact comprehensive computer crime legislation which created wholly new criminal actions.[111] Connecticut chose the latter approach.

While a prediction of how well the statute will meet the concerns

---

103. SOMA, *supra* note 2, at 288-95; Fiske, *White-Collar Crime: A Survey of Law*, 18 AM. CRIM. L. REV. 169, 384-86 (1980).

104. Comment, *supra* note 64, at 253; *see* Fiske, *supra* note 103, at 384-86 (citing trend in favor of admittance as exception to the hearsay and best evidence rules). *See also* J. WEINSTEIN, WEINSTEIN'S EVIDENCE ¶ 1001(4)[07] (1983) (contending that computer generated evidence should be admitted under existing rules); Connery and Levy, *Computer Evidence in Federal Courts*, 84 COM. L. J. 266 (1979) (arguing that computer evidence should be admitted under the Federal Rules of Evidence if the computer is shown to be reliable).

105. *See supra* note 58.

106. Each computer crime inflicts an average loss of approximately $450,000. PARKER, *supra* note 61, at 25. While the figure is skewed considerably by more recent, though infrequent, instances, Interim Proceedings, *supra* note 24, at 464, single strikes may range into the billions of dollars. PARKER, *supra* note 3, at 118; *see supra* notes 59-60 and accompanying text.

107. *See supra* notes 61-62 and accompanying text.

108. *See supra* note 63 and accompanying text.

109. *See supra* note 89.

110. *See supra* note 85 and accompanying text.

111. *See supra* note 89 and accompanying text.

of the drafters is premature,[112] the efforts of the drafters and of the Connecticut legislators have injected a demonstrably higher degree of certainty into Connecticut criminal law.

William S. Allred

112. No actions have arisen under the statute since it became effective. *See supra* note 1.