Western New England Law Review

Volume 7 *7 (1984-1985)*
Issue 3

Article 6

1-1-1985

LEGAL ANALYSIS OF ELECTRONIC BULLETIN BOARD ACTIVITIES

John T. Soma

Paula J. Smith

Robert D. Sprague

Follow this and additional works at: http://digitalcommons.law.wne.edu/lawreview

Recommended Citation

John T. Soma, Paula J. Smith, and Robert D. Sprague, *LEGAL ANALYSIS OF ELECTRONIC BULLETIN BOARD ACTIVITIES*, 7 W. New Eng. L. Rev. 571 (1985), http://digitalcommons.law.wne.edu/lawreview/vol7/iss3/6

This Article is brought to you for free and open access by the Law Review & Student Publications at Digital Commons @ Western New England University School of Law. It has been accepted for inclusion in Western New England Law Review by an authorized administrator of Digital Commons @ Western New England University School of Law. For more information, please contact pnewcombe@law.wne.edu.

LEGAL ANALYSIS OF ELECTRONIC BULLETIN BOARD ACTIVITIES

JOHN T. SOMA*
PAULA J. SMITH**
ROBERT D. SPRAGUE***

TABLE OF CONTENTS

I. INTRODUCTION

The popularity of the micro-computer, now most familiar to the public as the personal computer, has opened information processing and management to a new audience. The data processing industry for

* Associate Professor of Law, University of Denver College of Law. M.A., University of Illinois, 1973; J.D., University of Illinois, 1973; Ph.D., University of Illinois School of Commerce, 1975. Professor Soma recently published COMPUTER TECHNOLOGY AND THE LAW (1983 & Supp. 1984).

** Research Associate and J.D. Candidate, University of Denver College of Law. Paula has over ten years experience as a programmer/analyst in the data processing field and plans to specialize in Computer Law.

*** Research Associate and J.D. Candidate, University of Denver College of Law. Robert plans to specialize in Computer Law and is a hacker at heart.

years has recognized that data is only as good as its source and that a computer system's integrity is only as good as its security. This rubric of data processing is just making itself known to the new users among the general public. Each user access of a computer system represents another opportunity for compromise of the data base accessed.

One common method of linking micro-computers is referred to as networking. On a small scale, this can be accomplished through the telephone lines by connecting each computer to a modem.[1] The Electronic Bulletin Board System (BBS) is a computer software package that facilitates one method of networking. The BBS is used as a computerized information clearing house. BBSs allow users to send and receive messages concerning a variety of subjects from dog breeding, real estate listings, and computer programming tips to chess strategies and computer game participation.[2] There are an estimated 3,500-4,500 active BBSs nationwide.[3]

This article examines the potential liability of the BBS operator (known as a SYSOP) for information posted on a BBS and the use of such information by a BBS user.[4] Information relating to "phreaker" and "hacker" activities is of particular importance to this article since

---

1. A modem is a device through which computers can communicate. It is required at the sending and at the receiving locations. A modem converts electrical impulses into audible signals and vice versa. A sending computer sends its impulses into the modem, which converts them into audible signals and transmits the signals over telephone lines. The sounds are accepted by the receiving modem, converted back into electrical impulses, and sent to the receiving computer.

2. An Electronic Bulletin Board System (BBS) is a computer program which permits users to read and store messages. Although large, commercial data bases (*e.g.*, CompuServe) are a type of BBS, this article is concerned with those systems generally run on, and accessed by, micro-computers and which are operated by individuals as a hobby or by computer stores.

To access a BBS, one needs a terminal (generally a micro-computer such as an Apple, Commodore, TRS-80, or IBM-PC), a modem, and communications software. One can generally obtain a list of local BBSs from a local computer store, although there are now books on the market which list BBS numbers throughout the United States (see *infra* note 3).

Most BBSs contain a number of sub-boards. In this way, the user can actually access a number of boards (concerning a variety of topics) on just one BBS. Appendix A contains an edited printout of a BBS session that was conducted on a phreaker sub-board.

3. It is difficult to accurately estimate the number of active BBSs. Many BBSs are private. A user must generally know the SYSOP personally in order to obtain the telephone number for a private BBS and to gain access. The 1984 edition of a guide to underground BBSs estimates that there are over 1,500 active BBSs nationwide. T. BEESTON & T. TUCKER, HOOKING IN: THE UNDERGROUND COMPUTER BULLETIN BOARD WORKBOOK AND GUIDE (1984). The same guide, however, lists only 15 BBSs in the Denver area. *Id.* at 100 (p. 17 Supp.). The authors know of some 50-60 currently active BBSs in the Denver area alone.

4. "SYSOP" is an abbreviation for "systems operator."

these activities constitute the greatest potential source of liability for a SYSOP. A "phreaker" is someone who likes to play with the phone system. Phreakers have been active since at least the late 1960's.[5] They specialize in using telephone equipment for their own use, free of charge. Through devices (such as blue boxes), they make toll-free calls around the world.[6] When long-distance competition arrived and telephone credit codes began to proliferate, the phreakers had a whole new world opened up for them.[7]

Phreaker boards (BBS's or BBS sub-boards which specialize in phreaker information) include such items as diagrams for building blue boxes, telephone credit codes, and tips on how to avoid being caught (*e.g.*, which long-distance services can trace a call and how fast). This article will analyze state and federal laws pertaining to this type of information, specifically applied to the potential liability a SYSOP faces for posting phreaker information on the BBS.

In addition to the telephone system, computer systems have be-

---

5. See Rosenbaum, *Secrets of the Little Blue Box*, ESQUIRE, Oct. 1971, at 116 for an excellent insight into the world of phreakers. Although the article is over 13 years old, it remains highly accurate.

6. The blue box is one of the original phreaking devices. It is a small box (sometimes as small as a cigarette package) with 12 push buttons. The key to using a blue box is to touch certain buttons in order to create a 2600 cycle tone. A person calls a toll-free "800" number. Once the number starts ringing, but before someone answers, the box is used to send the 2600 cycle tone through the phone receiver. This disconnects the line at the destination, but keeps it open for the user. The user may then enter a number for anywhere in the United States. The billing system remains under the toll-free status.

Through deceit and additional devices, phreakers are now able to make toll-free calls around the world. They also use maintenance trunk lines to make toll-free conference calls. Some of the more sophisticated phreakers are beginning to experiment in accessing satellite transmissions. (These people refer to themselves as "satphrackers.").

7. Telephone credit card codes, as referred to in this article, are essentially a credit device through which a person may access long-distance telecommunications services and defer billing. Under AT&T's current system, the customer is assigned a credit code which is based on the customer's home or office telephone number, with additional coding numbers added. The customer merely enters this code via the telephone receiver's pushpad. Independent long-distance telecommunications services (such as MCI and Sprint) offer a slightly different variation. The customer dials a local number, enters his/her personal credit code (usually a five digit number) and then the number of the person to be called.

Phreakers have taken a liking to many of the independent long-distance services because of their lack of security. Once the local access number and corresponding credit code(s) were learned, a phreaker could use a code with little fear of being caught, until the long-distance service finally cancelled the code. Access numbers and credit codes are easy to discover with the use of a computer. First, the computer dials telephone numbers under certain prefixes (the long-distance service usually uses only one or two prefixes) and records the numbers which answered with a computer tone. Once these numbers are found, the phreaker tries five digit combinations until a call is able to be completed. (The use of computers by phreakers has led to a new category of phreakers and hackers, known as phrackers).

come an irresistible if not compulsive attraction for a new generation of electronic wizards known as "hackers." Hackers are computer hobbyists to the extreme. They have been around since the first days of the computer. They were originally some of the first college students to have access to computers and were known to be possessed with the idea of always perfecting computers and programs.[8] Today, the hacker is more commonly known as a person (often a juvenile) with a micro-computer who is trying to break into another computer. The goal of most of these hackers is just to get into that other computer system—to outsmart it. Once inside, they generally just browse around or leave a message to prove that they got inside. Occasionally, but not always intentionally, they damage data or the entire system. A few hackers are vandals and will go into a system for the sole purpose of bringing it down.[9]

A hacker board (a BBS or a BBS sub-board which specializes in hacker information) provides tips on how to penetrate computer systems as well as the phone numbers to computers and passwords. This article will focus on two aspects of hacker activity—the potential liability for a BBS SYSOP for posting hacker information and the protection a SYSOP may have if his or her own computer is attacked by someone.

II. OVERVIEW OF LEGAL ANALYSIS

This article will focus on the following specific activities: (1) unauthorized access, or attempted access, to computer systems; (2) the alteration, destruction, or damage to computer data or software, whether intentional or unintentional; (3) the destruction or damage to computer equipment, whether intentional or unintentional; (4) the interruption of, or impairment to, legitimate computer use by attempted unauthorized access or by vandalism (e.g., altering data, leaving obscene messages, tying up access channels, etc.); (5) obtaining telephone services without payment, whether through trick or device; (6) obtaining telephone services without payment through the unauthorized

8. See Levy, *Bummed to the Mimimum, Hacked to the Max*, ACCESS (Special Issue NEWSWEEK), 101 (Fall 1984) for a history of the hacker. *See also* Landreth, *Inside the Inner Circle*, Popular Computing 62 (May 1985), for an excellent insight into the world of the juvenile hacker. The article is adapted from the forthcoming book, LANDRETH, OUT OF THE INNER CIRCLE: A HACKER'S GUIDE TO COMPUTER SECURITY (1985).

9. "Bringing a system down" and "crashing a system" essentially mean to make the computer system stop working. Many times a hacker may bring a system down quite by accident, while others access a system with that sole purpose in mind. This is why any type of unauthorized access can have very serious consequences.

use of telephone credit codes; and (7) publishing telephone credit codes.

Unauthorized access may not appear on the surface to be of particular concern, but it can have serious consequences. If detected, unauthorized access destroys the credibility for the integrity of a computer system—especially one containing sensitive data. This could result in expending considerable amounts of managerial and technical resources to re-establish credibility in the system. There is always the additional risk of alteration, damage, or destruction to data or software, or damage or destruction of equipment, whether intentional or unintentional, associated with any unauthorized access.

Individual state computer-related statutes[10] have, therefore, been examined with a view toward provisions for unauthorized access alone. Where state computer-related statutes have no "access only" provisions, or do not exist at all, other statutory provisions which may be applicable to hacker activities have been examined. These state statutory provisions include private nuisances (interference with the use or enjoyment of property), criminal mischief (destruction of the property of another), and tampering (interference with the property of another). False pretenses and false impersonation statutes have also been examined since the hacker must generally achieve success through the use of a false or impersonated password. In addition, telephone harassment statutes have been analyzed. Since the hacker cannot gain the unauthorized access to the computer systems except by phone and the access is generally made by repeated attempts,[11] this would constitute repeatedly calling a number, whether or not conversation ensues, with no legitimate purpose of communication. Many state telephone harassment statutes contain this (or similar) language.[12]

Some hackers do attempt unauthorized access with the intent to

---

10. The types of statutes examined in this article are referred to as computer-related statutes. This phrase was chosen because of the different labels placed upon individual state computer-related statutes (*e.g.*, "Computer Fraud Statute," "Computer Crime Statute," "Computer Related Crimes Statute," "Computer Trespass Statute," etc.). "Computer-related statute" itself may also be a misnomer since many states' computer statutes may also be related to computer data bases maintained by the state, computerized educational services, etc. For purposes of this article, however, computer-related statutes refer to those statutes as qualified *infra*.

11. The computer systems which are vulnerable are those which have dial-up capabilities (*i.e.*, a computer which can be accessed via a telephone). A hacker usually gains entry by randomly entering passwords and usercodes and then focusing in on particular passwords and codes based on hints received from the computer system. This can often be a time-consuming project which requires repeated calls.

12. *See, e.g.*, ALA. CODE § 13A-11-8 (1975); ARK. STAT. ANN. § 41-2910 (1977).

commit theft or fraud. Therefore, where a state does not have a computer-related statute (or does have one but with no fraud or theft provisions), general theft and fraud statutes have been analyzed to determine whether their language possibly covers this type of hacker activity.

Phreaker activities have been more directly examined. They basically involve the theft of telecommunications services. Phreaker activities originally involved obtaining long-distance (within the U.S. or abroad) and teleconferencing services through the use of devices or deceit. Services were obtained by using devices which imitated telecommunications tones—manipulating telephone lines and cables.[13] Services were also obtained by deceiving telephone employees into believing the phreaker was a fellow maintenance employee, thereby convincing the employees to grant the phreaker access to special lines and cables.

Phreakers today have taken advantage of the recent break-up of AT&T and the subsequent proliferation of independent long-distance services, to make free long-distance calls. Phreakers utilize the telephone credit codes to make unauthorized calls.[14] More sophisticated phreakers use a combination of devices and telephone credit codes in order to avoid detection.

Many states have some type of "Theft of Telecommunications" statute. Most of the states which do not have such a statute include telecommunications under their theft of service statute. In addition, most states also provide for theft of telecommunications services by a device. These "device" statutes generally provide against possession, use, and sale of the device or plans and specifications to make such a device.[15] More directly related to BBS activities, many states have provisions for the publication of telephone credit codes and the plans for telecommunications theft devices.[16] There also exist specific federal statutes which directly relate to phreaker activities.[17]

Many hackers and phreakers are juveniles. The ability to prose-

---

13. This is usually accomplished through an array of devices such as blue boxes, black boxes, and silver boxes. *See supra* note 6.

14. *See supra* note 7.

15. *See, e.g.*, CAL. PENAL CODE § 502.7(b) (West Supp. 1984); IDAHO CODE § 18-6713(2) (Supp. 1984).

16. *See, e.g.*, IDAHO CODE § 18-6714 (Supp. 1984); ILL. ANN. STAT. ch. 134 § 15c (Smith-Hurd Supp. 1984-1985).

An example of a telecommunications theft device is the blue box. *See supra* notes 6 & 13. Various states use different language to describe these types of devices. For convenience, they will all be referred to as a telecommunications theft device in this article.

17. *See, e.g.*, 18 U.S.C. § 1343 (1982).

cute these individuals would, therefore, depend on individual state juvenile statutes. Statutes pertaining to parental liability for the crimes or torts of their children have, however, been reviewed for each state.

III. STATE COMPUTER CRIME AND TELECOMMUNICATIONS THEFT STATUTES

To date, thirty-five states have addressed computer crime in some manner. Six states have incorporated computer-related criminal activities into previously existing statutes, while twenty-nine states have passed some type of specific computer-related law. Following is a synopsis of laws for each state which may be applicable to BBS activities concerning hacker and phreaker information. (Appendix B contains a table illustrating an abbreviated analysis of state computer-related statutes. Appendix C contains a table illustrating an abbreviated analysis of state telecommunications fraud statutes).

Alabama

Computer crime is incorporated into Alabama's theft of service provisions where computer services are included in the definition of services.[18] Alabama has the following statutes which may be applicable to BBS/hacker related activities: criminal tampering in the second degree;[19] criminal mischief;[20] misrepresentations of material facts;[21] and telephone harassment.[22] Alabama also has a "prohibited instruments" provision.[23] In addition, Alabama has a statute providing for the liability of parents for the destruction of property by a minor.[24]

Alaska

In a prosecution for an offense that requires deception as an element, it is not a defense in Alaska that the defendant deceived or attempted to deceive a machine.[25] Under this provision, a machine is defined as, inter alia, a computer.[26] Additional potentially applicable statutes include private nuisance[27] and criminal mischief.[28] Alaska

18. ALA. CODE § 13A-8-10(b) (1975).
19. *Id.* § 13A-7-26.
20. *Id.* §§ 13A-7-21 to 23.
21. *Id.* § 6-5-101.
22. *Id.* § 13A-11-8.
23. *Id.* § 37-8-217 (1975).
24. *Id.* § 6-5-380.
25. ALASKA STAT. § 11.46.985 (1978).
26. *Id.*
27. *Id.* § 09.45.230.
28. *Id.* § 11.46.480.

also provides for the liability of parents for the destruction of property by minors.[29]

Arizona

There is a computer fraud statute[30] in Arizona which provides that (1) "[a] person commits computer fraud in the first degree by accessing, altering, damaging or destroying without authorization" any computer system with the intent (a) to "devise or execute any scheme or artifice to defraud or deceive," or (b) to "control property or services by means of false or fraudulent pretenses, representations or promises"[31] and (2) "[a] person commits computer fraud in the second degree by intentionally and without authorization accessing, altering, damaging or destroying" any computer system or any computer software, program or data contained in such computer system.[32] In addition, Arizona has a telecommunications fraud statute.[33] This statute prohibits the theft of telecommunications services through: (1) the unauthorized use of telephone credit codes, trick, or device;[34] (2) the publication (disclosure) of telephone credit codes;[35] and (3) the use, possession, sale, or transfer of a telecommunications theft device or the plans and specifications for making the same.[36]

Arkansas

Arkansas has no specific computer-related statute. Property is defined (under the theft provisions) as including tangible and intangible property.[37] The telephone harassment statute[38] may apply to BBS/hacker activities. Arkansas also provides for the liability of parents for the destruction of property by minors.[39] Arkansas has no specific telecommunications theft statute. The state's theft of services statute does, however, include telecommunications services.[40]

---

29. *Id.* § 34.50.020 (1975). Since the completion of this article, Alaska has passed a computer crime law. *See* ALASKA STAT. § 11.46.740 (1985). For applicable definitions, see *id.* § 11.46.990.

30. ARIZ. REV. STAT. ANN. § 13-2316 (1978).

31. *Id.* § 13-2316(A).

32. *Id.* § 13-2316(B).

33. *Id.* § 13-3707.

34. *Id.* § 13-3707(A)(1).

35. *Id.* § 13-3707(A)(2).

36. *Id.* § 13-3707(A)(3).

37. ARK. STAT. ANN. § 41-2201(6) (1977).

38. *Id.* § 41-2910.

39. *Id.* § 50-109 (Supp. 1983).

40. *Id.* § 41-2201(8) (1977).

California

The California computer crime statute prohibits access of any computer with the intent to defraud, as well as maliciously accessing, altering, deleting, damaging, or destroying any computer system, computer program, or data.[41] In addition, California has recently amended that statute to make intentional unauthorized access alone of any computer system, computer program, or data a misdemeanor and to provide a civil remedy for the owner or lessee of the computer system, computer program, or data.[42] California also has a statute pertaining to obtaining telephone services by fraud.[43] It includes the obtaining of telephone services, with intent to defraud, by unauthorized use of a telephone credit code, trick, or device. The statute also prohibits the manufacture, possession, sale, or transfer of a telecommunications theft device and the publication of telephone credit codes.[44]

Colorado

The Colorado computer crime statute prohibits the use of a computer for the purposes of theft of money, property, or services, or to defraud.[45] The statute also prohibits the unauthorized use, alteration, damage, or destruction of any computer system.[46] Although Colorado does not have a specific telecommunications theft statute, it does have a statute pertaining to illegal telecommunications equipment.[47] Colorado has recently passed a statute relating to a "financial transaction device," which is defined, inter alia, as a device that can be used to obtain services.[48] It is arguable that telephone credit codes could fall under this broad definition and, therefore, be included under this statute's provisions for unauthorized use.[49] Colorado also has a statute providing for parental liability for the crimes of minors.[50]

---

41. CAL. PENAL CODE § 502 (West Supp. 1984).

42. Act of Sept. 7, 1984, ch. 949, 1984 CAL. LEGIS. SERV. 298 (West) (amending CAL. PENAL CODE § 502 (West Supp. 1984)). *See* COMPUTER CRIME L. REP. (J.F.K. LIBRARY, CALIFORNIA STATE UNIVERSITY), I-5 (1984).

43. CAL. PENAL CODE § 502.7 (West Supp. 1984).

44. *Id.*

45. COLO. REV. STAT. § 18-5.5-102 (Supp. 1984).

46. *Id.*

47. *Id.* § 18-9-309 (1978).

48. *Id.* § 18-5-701 (Supp. 1984).

49. *Id.* § 18-5-702.

50. *Id.* § 18-1-801 (1978).

Connecticut

Connecticut has a far-reaching computer crime law[51] which (1) prohibits the (a) unauthorized access to a computer system;[52] (b) theft of computer services;[53] (c) interruption of computer services;[54] (d) misuse of computer system information;[55] and (e) destruction of computer equipment[56] and (2) provides for (a) the right of an aggrieved person to request appointment of a receiver who may, inter alia, seize the computer equipment of one who has violated this statute;[57] and (b) the right of an aggrieved person to bring a civil action against one who is alleged to have violated this statute.[58] Connecticut's harassment statute may also be applicable provided an intent to harass or annoy is proven.[59]

Connecticut does not have a specific telecommunications theft statute. Its theft of services statute does, however, include a provision related to obtaining telecommunications services, with intent to avoid payment by trick, code, or device.[60]

Delaware

The computer-related statutes in Delaware apply to computer fraud and computer misuse.[61] The revised statutes prohibit the knowing and unauthorized access of any computer system;[62] obtaining unauthorized computer services;[63] disruption or degrading of computer services or the denial of computer services to an authorized user;[64] the misuse of computer system information by (1) displaying, using, disclosing or copying data residing in, communicated by or produced by a computer system, or (2) altering, deleting, tampering with, damaging, destroying, or taking data intended for use by a computer system or interrupting or adding data to a computer system;[65] and the tam-

51. Act of May 31, 1984, Pub. Act. No. 84-206, 1984 CONN. LEGIS. SERV. 193 (West).
52. *Id.* § 2(b)(1).
53. *Id.* § 2(c).
54. *Id.* § 2(d).
55. *Id.* § 2(e).
56. *Id.* § 2(f).
57. *Id.* § 13.
58. *Id.*
59. CONN. GEN. STAT. § 53a-183 (1983).
60. *Id.* § 53a-119(7).
61. DEL. CODE ANN. tit. 11, §§ 931-39 (Supp. 1984).
62. *Id.* § 932.
63. *Id.* § 933.
64. *Id.* § 934.
65. *Id.* § 935.

pering with, taking, transferring, concealing, altering, damaging, or destroying of any computer equipment.[66] In addition, Delaware provides that an aggrieved person who has reason to believe that any other person has been engaged, is engaged, or is about to engage in an alleged violation of any provision the computer-related statutes may bring an action to: (1) temporarily or permanently restrain and enjoin the commencement or continuance of such acts; (2) order restitution; or (3) order the appointment of a receiver who may, inter alia, take into possession any property which belongs to the person who is alleged to have violated any of the above provisions.[67] Delaware does not have a specific telecommunications theft statute. It does, however, have a statute prohibiting the possession of, or dealing in, a device for unlawfully taking telecommunications services.[68] In addition, Delaware has a statute which prohibits the publication of credit cards or codes.[69] Although this statute does not specifically relate to telephone credit codes, Delaware's definition of a credit card includes, inter alia, evidence of an undertaking to pay for services.[70] In addition, Delaware has a statute providing for the recovery of damages from parents for the destruction of property by minors.[71]

District of Columbia

There is no specific computer-related or telecommunications theft statute in the District of Columbia. Its definition of property (under the theft provisions) includes tangible and intangible property.[72] The theft statute, however, includes the theft of telecommunications services.[73]

Florida

The Florida Computer-Related Crimes statute[74] prohibits the: (1) modification or destruction of data, programs or supporting documentation (with or without the intent to defraud);[75] (2) modification, destruction, or taking of computer equipment (with or without the in-

66. *Id.* § 936.
67. *Id.* § 939.
68. *Id.* § 850.
69. *Id.* § 903.
70. *Id.* § 904.
71. *Id.* tit. 10 § 3922.
72. D.C. CODE ANN. § 22-3801 (Supp. 1984).
73. *Id.* § 22-3811.
74. FLA. STAT. ANN. §§ 815.01-.07 (West Supp. 1984).
75. *Id.* § 815.04.

tent to defraud);[76] (3) unauthorized access of a computer system;[77] and (4) denial of computer system services to an authorized user.[78] Florida has a statute specifically prohibiting the theft of telecommunications services,[79] as well as the manufacture, sale, or transfer of a telecommunications theft device, or the plans and instructions to make the same.[80] In addition, Florida has a statute which prohibits the publication of telephone credit codes.[81] Florida also has a provision which permits civil actions against parents for the willful destruction or theft of property by minors.[82]

Georgia

The Georgia Computer Systems Protection Act[83] prohibits the knowing and willful, direct or indirect, unauthorized access, or attempted access, of any computer system for the purpose of: (a) "devising or executing any scheme or artifice to defraud;"[84] or (b) "obtaining money, property, or services . . . by means of false or fraudulent pretenses, representations or promises;"[85] and (2) the intentional and unauthorized, direct or indirect, access, alteration, damage, destruction, or attempted damage or destruction, of any computer system or any computer software, program or data.[86] Georgia has a statute that prohibits: (1) avoiding charges for the use of telephone services;[87] (2) the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same;[88] and (3) the publication of the plans or instructions for such device.[89] In addition, Georgia has a statute prohibiting the publication of telephone credit codes.[90]

Hawaii

There is no computer-related statute in Hawaii. There are, how-

76. *Id.* § 815.05.
77. *Id.* § 815.06.
78. *Id.*
79. *Id.* § 817.481 (West 1976).
80. *Id.* § 817.482-.483.
81. *Id.* § 817.483.
82. *Id.* § 741.24 (West Supp. 1984).
83. GA. CODE ANN. §§ 16-9-90 to -95 (1984).
84. *Id.* § 16-9-93(a)(1).
85. *Id.* § 16-9-93(a)(2).
86. *Id.* § 16-9-93(b).
87. *Id.* § 46-5-2 (Supp. 1984).
88. *Id.* § 46-5-3(a)(2) (1982).
89. *Id.* § 46-5-3(a)(3).
90. *Id.* § 16-9-39 (1984).

ever, statutes relating to criminal tampering in the second degree[91] and harassment[92] which may be applicable to BBS/hacker activities. Hawaii also has no specific telecommunications theft statute. Telecommunications services are, however, included as a service under the state's theft of services statute.[93] Hawaii has a statute which prohibits the manufacture, possession, use, sale, or transfer of a telecommunications theft device.[94]

Idaho

The Idaho Computer Crime statute[95] prohibits: (1) knowingly accessing, attempting to access, or using a computer system for the purpose of (a) "devising or executing any scheme or artifice to defraud," or (b) "obtaining money, property or services by means of false or fraudulent pretenses, represenations by promises;"[96] (2) knowingly and without authorization, altering, damaging, or destroying any computer system, computer software, program, documentation, or data;[97] and (3) knowingly and without authorization, accessing, or attempting to access, or using any computer system, computer software, program, documentation, or data.[98] Theft of telecommunications and telecommunications theft device provisions are contained in the same statute (which also includes theft by use of codes).[99] Idaho also has a provision relating to aiding in the avoidance of telecommunications charges that prohibits the publication of telephone credit codes.[100]

Illinois

The Illinois statute relating to the unlawful use of a computer[101] prohibits knowingly: (1) obtaining the use of a computer system without the consent of the owner;[102] (2) altering or destroying computer programs or data without the consent of the owner;[103] and (3) ob-

91. HAWAII REV. STAT. § 708-827 (1976).
92. *Id.* § 711-1106. Hawaii has just recently enacted a computer crime statute. *See* HAWAII REV. STAT. §§ 708.890 to -896 (1985).
93. *Id.* § 708-800.
94. *Id.* § 275-9 (Supp. 1983).
95. IDAHO CODE §§ 18-2201 to -2202 (Supp. 1984).
96. *Id.* § 18-2202(1).
97. *Id.* § 18-2202(2).
98. *Id.* § 18-2202(3).
99. *Id.* § 18-6713.
100. *Id.* § 18-6714.
101. Act of Sept. 11, 1979, § 1, ILL. ANN. STAT. ch. 38, § 16-9 (Smith-Hurd Supp. 1984-1985).
102. *Id.* § 16-9(b)(1).
103. *Id.* § 16-9(b)(2).

taining the use of, altering, or destroying a computer system as part of a deception for the purpose of obtaining money, property, or services from the owner of a computer system.[104] Illinois also has a statute relating to frauds concerning telecommunications services.[105] It prohibits obtaining telecommunications services, with intent to defraud, by the: (1) unauthorized use of telephone credit codes;[106] (2) use of a device;[107] (3) publication of telephone credit codes;[108] and (4) publication of plans, diagrams, or methods of construction for a telecommunications theft device.[109] Illinois also has a statute providing for parental liability for the damage to property by a minor.[110]

Indiana

There is no computer-related statute in Indiana. Other potentially applicable statutes include criminal mischief,[111] nuisance,[112] and harassment.[113] Indiana also has no specific telecommunications theft statute. Its deceptions statute, however, includes a prohibition against avoiding the lawful charge of telecommunications services by scheme or device.[114]

Iowa

Iowa has a statute relating to the crimes of unauthorized access, computer damage, and computer theft.[115] It prohibits knowingly and without authorization: (1) accessing a computer system; (2) damaging or destroying, or with the intent to injure or defraud, altering any computer system, computer software, or program; (3) accessing a computer system for the purpose of obtaining services, information, or property; and (4) with intent to deprive the owner permanently of possession, taking, transferring, concealing, or retaining possession of a computer system, computer software, program, or data.[116] No provi-

104. *Id.* § 16-9(b)(3).
105. Act of June 30, 1927, § 1, ILL. ANN. STAT. ch. 134, § 15c (Smith-Hurd Supp. 1984-1985).
106. *Id.* § 15c(1)(a).
107. *Id.* § 15c(1)(c).
108. *Id.* § 15c(1)(e).
109. *Id.* § 15c(1)(f).
110. Act of Oct. 6, 1969, §§ 1-7, ILL. ANN. STAT. ch. 70, §§ 51-57.
111. IND. CODE ANN. § 35-43-1-2 (Burns Supp. 1984).
112. *Id.* § 34-1-52-1 to -52-2 (Burns 1973).
113. *Id.* § 35-45-2-2 (Burns 1979).
114. *Id.* § 35-43-5-3(b) (Burns Supp. 1984).
115. Act of May 10, 1984, §§ 1-6, 1984 IOWA LEGIS. SERV. 11 (West) (to be codified at IOWA CODE § 716.A).
116. *Id.*

sion relating to the theft of telecommunications services was found for Iowa. Iowa does, however, have a statute that provides for parental responsibility for actions of children.[117]

Kansas

Kansas has no computer-related statute, but does have theft of services[118] and harassment by telephone[119] statutes which may potentially be applicable to BBS/hacker activities. The Kansas theft of telecommunications services statute[120] prohibits: (1) the manufacture or possession of a telecommunications theft device;[121] (2) selling or transferring such a device, or plans or instructions for assembling the same;[122] (3) publishing plans or instructions for a telecommunications theft device;[123] (4) publishing telephone credit codes;[124] (5) the unauthorized use of telephone credit codes;[125] and (6) avoiding charges for any telecommunication service by any fraudulent scheme, device, means or method.[126] In addition, Kansas provides civil remedies for a utility against anyone who publishes telephone credit codes or who obtains credit for, or purchases, any utility service by the unauthorized use of telephone credit codes.[127] Kansas also has a provision providing for the recovery from parents for malicious or willful acts by children.[128]

Kentucky

Although it has no computer-related statute, Kentucky does define property (under its theft provisions) as including tangible and intangible property.[129] Kentucky also has a criminal mischief statute which relates to the tampering or destroying of property.[130] In addition, Kentucky has a telecommunications theft device statute which

117. IOWA CODE ANN. § 613.16 (West Supp. 1984-85).
118. KANSAS STAT. ANN. § 21-3704 (1981).
119. *Id.* § 21-4113.
120. *Id.* § 21-3745.
121. *Id.* § 21-3745(1)(a).
122. *Id* § 21-3745(1)(b).
123. *Id.* § 21-3745(1)(c).
124. *Id.* § 21-3745(1)(d).
125. *Id.* § 21-3745(1)(e).
126. *Id.* § 21-3745(1)(f).
127. *Id.* § 66-1602 (Supp. 1983).
128. *Id.* § 38-120 (1981).
129. KY. REV. STAT. ANN. § 514.010(b) (Bobbs-Merrill Supp. 1984). Since the completion of this article, Kentucky has enacted a computer crime statute. *See* KY. REV. STAT. ANN. §§ 434.840 to -860 (1985).
130. *Id.* §§ 512.000-.040 (Bobbs-Merril 1975 & Supp. 1984).

prohibits the possession, use, sale, or transfer of such a device, or plans or instructions for making the same.[131]

Louisiana

Louisiana has a statute pertaining to computer related crime[132] which prohibits the: (1) intentional destruction, insertion, modification, disclosure, use, copying, taking, or accessing, without consent, of intellectual property (which is defined in the statute as, inter alia, computer software, programs, and data); (2) intentional modification or destruction, without consent, of computer equipment or supplies; (3) intentional denial to an authorized user, without consent, of the full and effective use of, or access to, a computer system; and (4) access of any computer system with the intent to defraud or obtain money, property, or services by means of false or fraudulent conduct, practices, or representations, or through the alteration, deletion, or insertion of programs or data.[133] Louisiana has a statute prohibiting the avoidance of payment for telecommunications services by the use of a code, a device, or by the use of any other fraudulent means, method, trick, or device.[134] Louisiana also has a statute prohibiting the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions to make or assemble the same.[135]

Maine

In Maine, the theft of computer and telephone services are incorporated into the state's theft of services statute.[136] Maine also has a statute prohibiting the possession, manufacture, or transfer of a device useful for advancing or facilitating the commission of the theft of services.[137] A statute potentially applicable to BBS/hacker activities is criminal mischief.[138] Property, under Maine's theft provisions, is defined as including tangible and intangible property.[139] In addition, Maine has a statute providing for the liability of parents for damage caused by children.[140]

---

131. *Id.* § 514.065 (Bobbs-Merrill Supp. 1984).

132. Act of July 13, 1984, § 1, 1984 LA. SESS. LAW SERV. 711 (West) (to be codified at LA. REV. STAT. §§ 14:73.1-:73.5).

133. *Id.*

134. LA. REV. STAT. ANN. § 14:221 (West Supp. 1984).

135. *Id.* § 14:222 (West 1974).

136. ME. REV. STAT. ANN. tit. 17-A, § 357 (1964).

137. *Id.* tit. 17-A, § 907.

138. *Id.* tit. 17-A, § 806.

139. *Id.* tit. 17-A, § 352(1).

140. *Id.* tit. 19, § 217.

Maryland

Maryland has two different types of computer-related statutes. Both are found under Maryland's crimes and punishments Article 27. The first statute relates to activities that are found under many computer crime statutes. It essentially prohibits the intentional, willful, and unauthorized access, or attempted access, of a computer system or computer software.[141] The second statute prohibits the willful making of a false entry, alteration, destruction, removal, concealment, or access of any public records.[142] Maryland has also included computer equipment and telecommunications services in its definitions of services under its theft provisions.[143] Furthermore, Maryland has a statute prohibiting the manufacture, sale, possession, or transfer of a telecommunications theft device, or the plans or instructions for making the same, as well as a statute prohibiting the publication of telephone credit codes.[144] In addition, Maryland has a statute providing for parental liability for the acts of a child.[145]

Massachusetts

In Massachusetts, the definition of a trade secret, under the larceny provisions, includes electronically processed or stored data, either tangible or intangible, and data while in transit.[146] Massachusetts also has statutes relating to: obtaining telecommunications services with the intent to defraud; manufacturing, possessing, using, selling, or transferring a telecommunications theft device, or the plans or instructions for making the same; and publishing telephone credit codes.[147] In addition, Massachusetts has a statute providing for parental liability for the willful acts of minor children.[148] The Massachusetts Senate has a proposed bill concerning electronic crime.[149] It would prohibit the willful, knowing, and unauthorized, with or without an intent to defraud, modification, destruction, disclosure, use, taking, or damaging of computer data, programs, or supporting documentation, or computer equipment or supplies, as well as the denial of

141. MD. CRIM. LAW CODE ANN. § 146 (Supp. 1984).
142. *Id.* § 45A.
143. *Id.* § 340(j) (1982).
144. *Id.* § 557A.
145. MD. CTS. & JUD. PROC. CODE ANN. § 3-829 (1984).
146. MASS. GEN. LAWS ANN. ch. 266, § 30 (West Supp. 1984-1985).
147. *Id.* ch. 166, § 42B (West Supp. 1984).
148. *Id.* ch. 231, § 85G.
149. MASS. LEG. DOC. NO. 240 (1984) (Senate bill proposal in 1984, currently pending before the 1985 Massachusetts Legislature). *See* COMPUTER CRIME L. REP., *supra* note 42 at II-73.

computer services to authorized users.[150] The proposed legislation also provides that the functional owner of the computer system shall be responsible for the protection of that resource by instituting acceptable physical security and computer system/network security controls to protect the user of those resources.[151]

The Massachusetts House of Representatives also has proposed computer-related legislation.[152] Its bill prohibits: (1) the direct or indirect access, or attempted access, of any computer system, computer software, program, or database with an intent to defraud; (2) the direct or indirect access, or attempted access, of any computer system, computer software, program, or database for the purpose of obtaining money, property, or services by means of (a) false or unauthorized access (including use of any card, code or other access device), or (b) fraudulent or unauthorized input of data or instructions, manipulation of data, or reprogramming of logic; (3) directly or indirectly altering, damaging or destroying any computer system, computer software, program, or database; (4) accessing, taking, transferring, concealing, obtaining, copying, or retaining possession of any computer system, computer equipment, computer software, program, or database; and (5) accessing, altering, damaging, or destroying any computer system, computer software, program, or database with the intent to prevent, or interfere with, access by authorized users.[153]

Michigan

The computer-related statute[154] in Michigan prohibits: (1) access to a computer system "for the purpose of devising or executing a scheme or artifice with intent to defraud or for the purpose of obtaining money, property, or a service by means of a false or fraudulent pretense, representation, or promise;"[155] and (2) the intentional and unauthorized access, alteration, damage, or destruction of a computer system, computer software, program, or data.[156] The statute also prohibits the utilization of a computer system to commit a violation of other sections of the Michigan code.[157] Michigan also has statutes re-

150. MASS. LEG. DOC. NO. 240 (1984).

151. *Id.*

152. MASS. LEG. DOC. NO. 4844 (1984) (House bill proposal in 1984, currently pending before the 1985 Massachusetts Legislature). *See* COMPUTER CRIME L. REP., *supra* note 42 at II-85.

153. MASS. LEG. DOC. NO. 4844 (1984).

154. MICH. COMP. LAWS ANN. § 752.791-797 (West Supp. 1984).

155. *Id.* § 752.794.

156. *Id.* § 752.795.

157. *Id.* § 752-796.

lating to theft of telecommunications services which prohibit: knowingly obtaining, or attempting to obtain, "by the use of any fraudulent scheme, device, means, or methods, . . . telephone service with intent to avoid payment of charges therefor;"[158] obtaining telephone service by unauthorized use of telephone credit codes;[159] and the manufacture, possession, use, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same.[160]

Minnesota

Minnesota has computer crime statutes[161] which prohibit the: (1) intentional and unauthorized damage or destruction of any computer system or computer software;[162] (2) intentional and unauthorized alteration of any computer system or computer software, with the intent to injure or defraud;[163] (3) intentional and unauthorized, or without claim of right, accessing of any computer system for the purpose of obtaining services or property;[164] and (4) intentional, and without claim of right, and with intent to permanently deprive the owner of possession, taking, transferring, concealing, or retaining possession of any computer system, computer software or data.[165]

Minnesota's computer crime statute does not prohibit unauthorized access alone. Therefore, its obscene or harassing telephone calls statute[166] may be applicable. It prohibits the making of a telephone call, whether or not conversation ensues, without disclosing identity[167] and for making the telephone of another repeatedly ring.[168] Both of these provisions, however, require an intent to annoy or harass any person at the called number.[169] Minnesota has a statute relating to fraudulent long distance telephone calls.[170] It prohibits obtaining long distance telephone service by means of unauthorized use of telephone credit codes or through the manufacture, possession, use, or sale of a telecommunications theft device, or the plans or component parts for

158. *Id.* § 750.219c (West 1980).
159. *Id.* § 750.219a.
160. *Id.* § 750.540c (West Supp. 1984-1985).
161. MINN. STAT. ANN. §§ 609.87 -.89 (West Supp. 1984).
162. *Id.* § 609.88(1)(a).
163. *Id.* § 609.88(1)(b).
164. *Id.* § 609.89(1)(a).
165. *Id.* § 609.89(1)(b).
166. *Id.* § 609.79 (West 1964 & Supp. 1984).
167. *Id.* § 609.79(1)(b) (West Supp. 1984).
168. *Id.* § 609.79(1)(c).
169. *Id.* § 609.79(1).
170. *Id.* § 609.785 (West Supp. 1984).

the same.[171]

Mississippi

There is no computer-related statute in Mississippi. One statute which potentially may be applicable is malicious mischief which provides for the malicious injury or destruction of real or personal property of another.[172] Mississippi does, however, have a statute relating to theft of telecommunications services.[173] It prohibits obtaining services through the use of telephone credit codes and the obtaining of telephone services by the use of any fraudulent scheme, device, means, or method.[174]

Missouri

The Missouri computer tampering statute[175] prohibits knowingly and without authorization, with or without an intent to defraud: (1) modifying or destroying data, programs or supporting documentation;[176] (2) disclosing or taking confidential data, programs or supporting documentation;[177] (3) modifying, destroying, damaging, or taking computer equipment;[178] (4) destroying, damaging, or taking any computer system;[179] (5) accessing any computer system;[180] and (6) denying computer system services to an authorized user.[181] No statute relating to theft of telecommunications services could be found for Missouri. There is, however, a broad definition of credit devices which may be applicable to some BBS/phreaker activities. The statute's definition of a credit device includes a writing or number purporting to evidence an undertaking to pay for services rendered.[182] In addition, the statute relating to the fraudulent use of a credit device prohibits, inter alia, obtaining services through unauthorized use.[183] Missouri also has a statute providing for parental liability for damages caused by a

171. *Id.*
172. MISS. CODE ANN. § 97-17-67 (1972).
173. *Id.* § 97-19-31.
174. *Id.*
175. MO. ANN. STAT. §§ 569.093 -.099 (Vernon Supp. 1985).
176. *Id.* § 569.095.
177. *Id.*
178. *Id.* § 569.097.
179. *Id.*
180. *Id.* § 569.099.
181. *Id.*
182. *Id.* § 570.010(5) (Vernon 1979).
183. *Id.* § 570.130.

minor.[184]

Montana

Montana has a statute pertaining to the unlawful use of a computer.[185] It prohibits knowingly: (1) obtaining the use of any computer system without consent of the owner; (2) altering or destroying a computer program or software without consent of the owner; and (3) obtaining the use of, altering, or destroying a computer system for the purpose of obtaining money, property, or computer services.[186] Montana has two statutes relating to theft of telecommunications services. The first prohibits obtaining communication services with intent to defraud by means of: (1) using a code or prearranged scheme; (2) acoustically tampering with any equipment; (3) any other trick, stratagem, impersonation, false pretense, false representation, false statement, contrivance, device, or means; and (4) making, assembling or possessing a telecommunications theft device or the plans or instructions for making the same.[187] The second statute pertains to aiding the avoidance of telecommunications charges. It prohibits the: (1) publication of telephone credit codes; (2) publication, advertisement, sale, or transfer of the plans or instructions for making a telecommunications theft device; and (3) manufacture, possession, sale, or transfer of a telecommunications theft device.[188]

Nebraska

Although Nebraska has no computer-related statute, under its theft provisions, Nebraska defines property as including tangible and intangible property.[189] Potentially applicable statutes include: theft by deception;[190] theft of services;[191] and criminal mischief.[192] Nebraska's theft of services statute provides for telephone services.[193] The statute also prohibits the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same.[194]

---

184. *Id.* § 537.045 (Vernon Supp. 1985).
185. MONT. CODE ANN. § 45-6-311 (1983).
186. *Id.*
187. *Id.* § 45-6-306.
188. *Id.* § 45-6-307.
189. NEB. REV. STAT. § 28-509(5) (1979).
190. *Id.* § 28-512.
191. *Id.* § 28-515.
192. *Id.* § 28-519.
193. *Id.* § 28-515.
194. *Id.*

Nevada

The Nevada statute pertaining to the unlawful use of computers prohibits knowingly, willingly and without authorization, with or without an intent to defraud: (1) modifying, destroying, disclosing, using, taking, copying, or entering computer data, programs, or supporting documents; (2) modifying, destroying, using, taking, or damaging computer equipment or supplies; (3) destroying, damaging, or taking a computer system; and (4) denying the use of a computer system to an authorized user.[195] Nevada has a statute relating to fraudulently obtaining telecommunications services, which includes prohibitions for the unauthorized use of telphone credit codes.[196] In addition, Nevada has a statute prohibiting the manufacture, possession, sale, or transfer of a telcommunications theft device, or the plans or instructions for making the same.[197] Nevada also has a statute providing for civil liability of parents for a minor's willful misconduct resulting in property damage.[198]

New Hampshire

There is no computer-related statute in New Hampshire. Other potentially applicable statutes include: criminal mischief,[199] tampering;[200] theft of services;[201] and harassment.[202] In addition, New Hampshire's theft provisions define property as including tangible and intangible property.[203] New Hampshire's theft of services statute also defines services as including telephone services.[204] Furthermore, New Hampshire has a statute relating to fraudulent communications paraphernalia.[205] It prohibits the possession, manufacture, or transfer of a telcommunications theft device, or information for making the same, as well as communicating telephone credit codes.[206]

New Jersey

New Jersey currently has no computer-related statute. Statutes

195. NEV. REV. STAT. § 205.473-.477.
196. *Id.* § 205.480.
197. *Id.* § 205.490 (1967).
198. *Id.* § 41.470 (1979).
199. N.H. REV. STAT. ANN. § 634:2 (1974).
200. *Id.* § 638:3.
201. *Id.* § 637:8 (1974 & Supp. 1983).
202. *Id.* § 644:4 (1974).
203. *Id.* § 637:2.
204. *Id.* § 637:8.
205. *Id.* § 638:5a (Supp. 1983).
206. *Id.*

that may be applicable to BBS/hacker activities include theft of services,[207] theft by deception,[208] and wrongful impersonating.[209] In addition, New Jersey's theft of service statute includes obtaining telephone services by mechanical or electronic devices or through fraudulent statements.[210] New Jersey also has a statute providing for the liability of a parent for willful destruction of property by a minor.[211]

New Jersey has two proposed computer-related bills. The Senate bill would prohibit knowingly and without authority, directly or indirectly: (1) accessing any computer system for the purpose of the transfer of electrical impulses or the introduction of fraudulent data, database, records, computer software, or program with the intent to device or execute any scheme or artifice (a) to defraud or deceive, or (b) for monetary or financial gain by means of false or fraudulent pretenses, representations, or promises; (2) accessing, altering, damaging or destroying any computer equipment, computer system, computer program, or data, for the purpose of causing injury; (3) disclosing proprietary data, computer software, or programs; and (4) accessing any computer systems for the purpose of obtaining computer services for monetary or financial gain.[212] The New Jersey Assembly bill prohibits knowingly: (1) accessing any computer system for the purpose (a) of devising or executing any scheme or artifice to defraud or extort, (b) of obtaining money, property or services with the purpose to deceive or injure anyone, or (c) to conceal any wrongdoing; (2) accessing any computer system for the purpose of obtaining or altering unauthorized credit information; (3) accessing, altering, deleting, damaging, or destroying any computer system, computer program, or data; and (4) directly or indirectly disclosing proprietary data, computer software, or programs.[213]

New Mexico

The New Mexico statute relating to computer crimes prohibits: (1) accessing any computer system with the intent to (a) devise or execute any scheme or artifice to defraud, or (b) with the intent to obtain,

---

207. N.J. STAT. ANN. § 2C:20-8 (West Supp. 1984-1985).

208. *Id.* § 2C:20-4 (West 1982).

209. *Id.* § 2C:21-17.

210. *Id.* § 2C:20-8 (West Supp. 1984-1985).

211. *Id.* § 2A:53A-15.

212. N.J. LEG. DOC. No. 345 (1984) (proposed Senate bill). *See* COMPUTER CRIME L. REP., *supra* note 42, at II-96.

213. N.J. LEG. DOC. No. 29 (1984) (proposed Assembly bill). *See* COMPUTER CRIME L. REP., *supra* note 42, at II-100.

by means of embezzlement or false or fraudulent services; and (2) intentionally, maliciously, and without authorization, accessing, altering, damaging, or destroying any computer system.[214] New Mexico has statutes relating to theft of telecommunications services.[215] The statutes prohibit obtaining telecommunications services, with the intent to defraud, by unauthorized use of telephone credit codes or by using any other contrivance, device, or means.[216] The statutes also prohibit the manufacture, possession, sale, or transfer of a telecommunications theft device.[217] New Mexico also has a statute providing for parental liability for the damage or destruction of property by a child.[218]

New York

There is no computer-related statute in New York. Potentially applicable statutes include: criminal mischief;[219] criminal tampering in the second degree;[220] reckless endangerment of property;[221] and criminal impersonation.[222] New York's theft of services statute includes telephone services.[223] The statute prohibits obtaining telephone services by use of a telecommunications theft device or by an artifice, trick, deception, code, or device.[224] New York also has a statute providing for the liability of parents for the malicious and destructive acts of infants.[225]

North Carolina

The North Carolina statutes pertaining to computer-related crime[226] provide for the willful, direct or indirect, with or without the intent to defraud, accessing of any computer system,[227] and for the willful and unauthorized alteration, damage, or destruction of any computer system, computer software, program, or data.[228] North

214. N.M. STAT. ANN. § 30-16(A)-1 to -4 (1984).
215. *Id.* § 30-33-12 to -14 (1980).
216. *Id.* § 30-33-13(A).
217. *Id.* § 30-33-13(B).
218. *Id.* § 32-1-46 (Supp. 1984).
219. N.Y. PENAL LAW §§ 145.00 -.12 (McKinney 1975).
220. *Id.* § 145.15.
221. *Id.* § 145.25.
222. *Id.* § 190.25 (McKinney 1975 & Supp. 1984-1985).
223. *Id.* § 165.15.
224. *Id.*
225. N.Y. GEN. MUN. LAW § 78-a (McKinney Supp. 1984-1985).
226. N.C. GEN. STAT. § 14-453 to -457 (1981).
227. *Id.* § 14-454.
228. *Id.* § 14-455.

Carolina has no statutes relating to theft of telecommunications services. There is a general statute that prohibits avoiding charges for telephone services.[229] Another statute specifically prohibits the unauthorized use of telephone credit codes.[230] There is also a third statute which prohibits: (1) the manufacture, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same; (2) publishing the plans or instructions for making a telecommunications theft device; and (3) publishing telephone credit codes.[231]

North Dakota

The North Dakota computer fraud statute[232] prohibits (1) the unauthorized access, alteration, damage, or destruction of any computer system "with the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses, representations, or promises,"[233] and (2) the intentional, unauthorized access, alteration, damage, or destruction of any computer system, computer software, program, or data.[234] North Dakota has a statute which prohibits the manufacture, possession, sale, or transfer of a telecommunications theft device, or the offer or advertisement of such device for sale, or the plans or instructions for making the same.[235] North Dakota also has a statute prohibiting the unlawful publication of telephone credit codes.[236] In addition, North Dakota has a statute providing for parental liability for minor children.[237]

Ohio

Ohio is included as a state which has a specific computer-related statute. Its theft provisions include definitions directly related to computers.[238] There are, however, no other computer crime provisions in the Ohio code. Statutes that may be applicable to BBS/hacker activities include tampering with records[239] and criminal mischief.[240] Ohio

229. *Id.* § 14-113.4.
230. *Id.* § 14.113.3.
231. *Id.* § 14.113.5.
232. N.D. CENT. CODE § 12.1-06.1 -08 (Supp. 1983).
233. *Id.* 12.1-06.1-08(1).
234. *Id.* 12.1-06.1-08(2).
235. *Id.* § 8-10-07.2 (1975).
236. *Id.* § 8-10-07.3.
237. *Id.* § 32-03-39.
238. OHIO REV. CODE ANN. § 2913.01 (Page Supp. 1983).
239. *Id.* § 2913.42 (Page 1982).
240. *Id.* § 2909.07.

has a statute prohibiting the fraudulent use of telephone service (including unauthorized use of telephone credit codes)[241] and a statute prohibiting the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same.[242] In addition, Ohio has a statute providing for the liability of parents for the destructive acts or theft by their children.[243]

Oklahoma

The Oklahoma computer crime statute prohibits: (1) willfully, and without authorization, gaining access to and damaging, modifying, altering, destroying, copying, disclosing, or taking possession of a computer system; (2) using a computer system for the purpose of devising or executing a scheme or artifice with the intent (a) to defraud or (b) for the purpose of obtaining money, property, services, or other thing of value by means of a false or fraudulent pretense or representation; (3) willfully exceeding the limits of authorization and damaging, modifying, altering, destroying, copying, disclosing, or taking possession of a computer system; and (4) willfully and without authorization, gaining, or attempting to gain, access to a computer system.[244] Oklahoma has a statute which prohibits unlawfully obtaining telecommunications services (including the unauthorized use of telephone credit codes).[245] In addition, Oklahoma has a statute prohibiting the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same.[246] Oklahoma also has a statute that prohibits the publication of telephone credit codes.[247] Furthermore, Oklahoma has a provision for the recovery of damages from the parents of minors.[248]

Oregon

There is no computer-related statute in Oregon, although the theft of services statute may be applicable since it includes professional services under its definition of services.[249] Oregon does incorporate

241. *Id.* § 4931.32 (Page 1977).
242. *Id.* § 4931.33.
243. *Id.* § 3109.09 (Page 1980).
244. Computer Crimes Act, ch. 70, § 3, 1984 OKLA. SESS. LAW SERV. 245, 246 (West).
245. OKLA. STAT. ANN. tit. 21, § 1515 (West 1983).
246. *Id.* § 1516.
247. *Id.* § 1522.
248. *Id.* tit. 23, § 10 (West Supp. 1984).
249. OR. REV. STAT. §§ 164.005, 164.125 (1983).

telephone services into its theft of services statute.[250] In addition, Oregon has a statute prohibiting the possession of a fraudulent communications device.[251] Oregon also has a statute providing for the liability of parents for the torts committed by their child.[252]

Pennsylvania

The Pennsylvania statute pertaining to the unlawful use of a computer prohibits: (1) the access, alteration, damage, or destruction of any computer system, computer software, program, or data with the intent to (a) interrupt the normal functioning of an organization, (b) devise or execute any scheme or artifice to defraud or deceive, or (c) control property or services by means of false or fraudulent pretenses, representations, or promises, and (2) intentionally and without authorization, accessing, altering, damaging, or destroying any computer system, computer software, program, or data.[253] Pennsylvania has a statute prohibiting the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same.[254] Pennsylvania also has a provision that prohibits the publication of credit card numbers, wherein credit card is defined as, inter alia, a writing or number or other evidence of an undertaking to pay for services rendered.[255] In addition, Pennsylvania has a statute providing for parental liability for the torts of a child.[256]

Rhode Island

The computer crime statute[257] in Rhode Island prohibits: (1) the direct or indirect access of any computer system "for the purpose of (1) devising or executing any scheme or artifice to defraud or (2) obtaining money, property or services by means of false or fraudulent pretenses, representations, or promises;"[258] (2) intentionally and without authorization, directly or indirectly accessing, altering, damaging, or destroying any computer system, computer software, program, or data;[259] and (3) "intentionally and without claim of right, and with intent to permanently deprive the owner of possession," taking, trans-

250. *Id.* § 164.130.
251. *Id.* § 165.070.
252. *Id.* § 30.765.
253. 18 PA. CONS. STAT. ANN. § 3933 (Purdon Supp. 1984-1985).
254. *Id.* § 910 (Purdon 1983).
255. *Id.* § 4106.
256. PA. CONST. STAT. ANN. § 2002 (Purdon Supp. 1984-1985).
257. R.I. GEN. LAWS § 11-52-1 to -5 (1981 & Supp. 1984).
258. *Id.* § 11-52-2 (Supp. 1984).
259. *Id.* § 11-52-3.

ferring, concealing, or retaining possession of any computer system, computer software, program, or data.[260] Rhode Island has a statute that prohibits the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or specifications for making the same.[261] In addition, Rhode Island has a statute prohibiting the publication of telephone credit codes.[262] Rhode Island also has a statute providing for parental liability for torts of minors.[263]

South Carolina

There is no computer-related statute in South Carolina. There is, however, a statute prohibiting the avoidance of payment for telecommunications services through the unauthorized use of telephone credit codes or by, inter alia, the use of any other fraudulent means, method, trick, or device.[264] South Carolina also has a statute providing for parental liability for the malicious injury to property by a minor.[265]

South Dakota

The South Dakota statutes providing for the unlawful use of a computer[266] prohibit knowingly: (1) obtaining the use of a computer system without the consent of the owner;[267] (2) altering or destroying a computer program or data without the consent of the owner;[268] and (3) obtaining the use of, altering, or destroying a computer system "as part of a deception for the purpose of obtaining money, property, or services from the owner of a computer system or any third party."[269] South Dakota has a statute that prohibits obtaining telephone service without payment, which includes the unauthorized use of telephone credit codes.[270] South Dakota also has a statute which prohibits the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same.[271] In

260. *Id.* § 11-52-4.
261. *Id.* § 11-35-25.
262. *Id.* § 11-49-6.1 (1981).
263. *Id.* § 9-1-3 (Supp. 1984).
264. S.C. CODE ANN. §§ 16-13-400 to -410 (Law. Co-op. 1976).
265. *Id.* § 20-7-340 (Law. Co-op Supp. 1983). South Carolina has just recently passed a computer crime statute which is the first such legislation to contain a definition of "computer hacking." *See* S.C. CODE ANN. §§ 16-16-10 to -40 (1985).
266. S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to -8 (Supp. 1984).
267. *Id.* § 43-43B-1(1).
268. *Id.* § 43-43B-1(2).
269. *Id.* § 43-43B-1(3).
270. *Id.* § 49-31-37 (1983).
271. *Id.* § 49-31-36.

addition, South Dakota has a statute providing for parental liability for the willful acts of a child.[272]

Tennessee

The Tennessee computer crimes statutes[273] prohibit: (1) knowingly and willfully, directly or indirectly, accessing, or attempting to access, any computer system, computer software, program, or data for the purpose of (a) "devising or executing any scheme or artifice to defraud"[274] or (b) "obtaining money, property, or services . . . by means of false or fraudulent pretenses, representations, or promises;"[275] and (2) intentionally and without authorization, directly or indirectly, accessing, altering, damaging, destroying, or attempting to damage or destroy, any computer system, computer software, program, or data.[276] Tennessee has a statute that prohibits obtaining telephone service by fraudulent means.[277] In addition, Tennessee has a statute prohibiting the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same.[278] Tennessee also has a statute providing for recovery against parents for the property damage caused by a juvenile.[279]

Texas

There is no computer-related statute in Texas. Statutes which may be applicable to BBS/hacker activities include theft of services[280] and criminal mischief.[281] Texas does have a statute relating to fraudulently obtaining telecommunications services[282] which prohibits the publication of telephone credit codes[283] and the manufacture or possession of "any equipment specifically designed to be used to fraudulently avoid charges for telecommunications services."[284] Texas also has a statute providing for liability of parents for the conduct of a

272. *Id.* § 25-5-15 (1984).
273. TENN. CODE. ANN. §§ 39-3-1401 to -1406 (Supp. 1984).
274. *Id.* § 39-3-1404(a)(1).
275. *Id.* § 39-3-1404(a)2).
276. *Id.* § 39-3-1404(b).
277. *Id.* § 39-3-935 (1982).
278. *Id.* § 39-3-936.
279. *Id.* § 37-10-101 (1984).
280. TEX. PENAL CODE ANN. § 31.04 (Vernon Supp. 1984).
281. *Id.* § 28.03.
282. TEX. STAT. ANN. art. 1446(b) (Vernon 1980).
283. *Id.* art. 1446(b)(1).
284. *Id.* art. 1446(b)(2).

child.[285]

Utah

In Utah, computer fraud applies to:

> [A]ny person who willfully gains access to any . . . computer system, . . . computer software, [or] . . . program or knowingly and willfully provides false information or who causes any other person directly or indirectly to enter false information into any . . . computer system, . . . computer software [or] . . . program, and thereby devises or executes any scheme or artifice to defraud or obtain money, property or services, including the unauthorized use of computer time, under false pretenses, representations, or promises, including representations made to a computer, and thereby alters, damages or destroys any computer system, . . . computer software [or] . . . program.[286]

Since Utah's computer fraud statute does not specifically prohibit unauthorized access alone, other potentially applicable statutes must be considered, including criminal mischief,[287] tampering with records,[288] and telephone harassment.[289] Utah has a statute which provides for the theft of telecommunications services,[290] as well as for telecommunications theft devices.[291] Utah also has a statute providing for parental liability for property damage caused by a minor.[292]

Vermont

There is no computer-related statute in Vermont. Other potentially applicable statutes include: unlawful mischief;[293] false impersonation;[294] and false pretenses.[295] Vermont does have a statute relating to fraud against the owners of communications systems, which prohibits the unauthorized use of telephone credit codes.[296] Vermont also has a statute providing for parental liability for damages caused by a

---

285. TEX. FAM. CODE ANN. § 33.01 (Vernon 1975).

286. UTAH CODE ANN. §§ 76-6-703 (Supp. 1983). For the full Computer Fraud Act, see *id.* §§ 76-6-701 to -704.

287. *Id.* § 76-6-106 (1978).

288. *Id.* § 76-6-504.

289. *Id.* § 76-9-201.

290. *Id.* § 76-6-409.

291. *Id.* § 76-6-409.1 (Supp. 1983).

292. *Id.* § 78-11-20 (1953).

293. VT. STAT. ANN. tit. 13, § 3701 (1974).

294. *Id.* § 2001.

295. *Id.* § 2002 (Supp. 1983).

296. *Id.* § 2021 (1974).

minor.[297]

Virginia

The computer crimes statutes[298] in Virginia prohibit the unauthorized use of a computer with the intent to: (1) "obtain property or services by false pretenses,"[299] "embezzle or commit larceny,"[300] or "convert the property of another;"[301] (2) "temporarily or permanently remove computer data, . . . programs, or . . . software from a computer,"[302] "cause a computer to malfunction,"[303] "alter or erase any computer data, . . . programs, or . . . software,"[304] "effect the creation or alteration of a financial instrument or of an electronic transfer of funds,"[305] or "cause physical injury to the property of another;"[306] (3) examine "any employment, salary, credit or any other financial or personal information relating to any other person with the intent to injure such person;"[307] (4) "obtain computer services without authority;"[308] or (5) "cause physical injury to an individual."[309] In addition, Virginia's computer crime statute has a provision allowing the recovery of civil damages for any person whose property or person is injured by reason of a violation of any provision of this article.[310] Virginia also has a statute which prohibits telephone services without payment "by the use of any scheme, device, means or method."[311] In addition, Virginia has statutes which provide for an action against a parent for the damage to public or private property caused by a minor.[312]

Washington

Washington has a computer trespass statute.[313] It provides for

297. *Id.* tit. 15, § 901.
298. VA. CODE § 18.2-152.1 to -152.14 (Supp. 1984).
299. *Id.* § 18.2-152.3(1).
300. *Id.* § 18.2-152.3(2).
301. *Id.* § 18.2-152.3(3).
302. *Id.* § 18.2-152.4(1).
303. *Id.* § 18.2-152.4(2).
304. *Id.* § 18.2-152.4(3).
305. *Id.* § 18.2-154.4(4).
306. *Id.* § 18.2-154.4(5).
307. *Id.* § 18.2-152.5.
308. *Id.* § 18.2-152.6.
309. *Id.* § 18.2-152.7.
310. *Id.* § 18.2-152.12.
311. *Id.* § 18.2-187.1 (1982).
312. *Id.* §§ 8.01-43 to -44 (1984).
313. WASH. REV. CODE ANN. §§ 9A.52.110-.130 (Supp. 1985).

intentionally and without authorization gaining access to a computer system or data, with or without the intent to commit another crime.[314] Washington has a statute relating to fraudulently obtaining telephone service which prohibits the manufacture, possession, sale, or transfer of a telecommunications theft service, or the plans or instructions for making the same.[315] In addition, Washington has a statute prohibiting the publication of telephone credit codes.[316] Washington also has a statute providing for an action against a parent for the willful injury to persons or property by a minor.[317]

West Virginia

There is no computer-related statute in West Virginia. There is, however, a statute which prohibits obtaining services through the unauthorized use of telephone credit codes.[318] In addition, West Virginia has a statute prohibiting the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions for making the same.[319] West Virginia has a statute providing for parental liability for the willful, malicious, or criminal acts of children.[320]

Wisconsin

The Wisconsin computer crime statute prohibits: (1) the willful, knowing, and unauthorized modification, destruction, access, taking possession, or copying of data, computer programs, or supporting documentations and (2) the willful, knowing and unauthorized modification, destruction, use, taking, or damaging of a computer system, computer equipment, or supplies.[321] In addition, there is a provision which allows a judge to place restrictions on the offender's use of computers.[322] Wisconsin has a telecommunications fraud statute.[323] It also has a statute providing for parental liability for the acts of a minor child.[324]

---

314. *Id.*
315. *Id.* 9.45.240.
316. *Id.* § 9.26A.090 (1977).
317. *Id.* § 4.24.190 (1985).
318. W. VA. CODE § 61-3-24a (1984).
319. *Id.* § 61-3-24b.
320. *Id.* § 55-7A-2.
321. WIS. STAT. ANN. § 943.70 (West 1984 Supp. 1984-1985).
322. *Id.* § 943.70(4).
323. *Id.* § 943.45 (West 1982).
324. *Id.* § 895.035 (West 1983).

Wyoming

The computer crime statutes[325] in Wyoming prohibit knowingly and without authorization: (1) modifying, destroying or disclosing data, programs, or supporting documentation;[326] (2) modifying computer equipment or supplies;[327] and (3) accessing a computer system or denying computer system services to an authorized user.[328] Wyoming has a statute which prohibits fraudulently obtaining telecommunications services by an unauthorized use of telephone credit codes, or "by any other trick, strategem, impersonation, false pretense, false representation, false statement, contrivance, device, or means."[329] In addition, Wyoming has a statute which prohibits the manufacture, possession, sale, or transfer of a telecommunications theft device, or the plans or instructions to make the same.[330] Wyoming also has a statute providing for parental tort liability for the property damage by certain minors.[331]

IV. STATE COMPUTER CRIME PENALTIES

Unauthorized computer access has been the focus of discussion thus far. Penalties associated with such activity will now be examined. The majority of the twenty-nine states which have a specific computer-related statute provide that violations of the statutory sections which prohibit unauthorized access only are misdemeanors. Some of the states grade the offense: a violation is a felony if the resulting damage is greater than a certain amount (or if the violation is the result of a scheme or artifice to defraud). Five of the states, however, provide that any unauthorized access is a felony.[332] Three additional states do not specify whether a penalty is a misdemeanor or a felony, but provide for rather harsh consequences: Tennessee provides that unauthorized access may be punishable by a fine not exceeding $50,000 or imprisonment of not less than three years or not more than ten years, or both;[333] Louisiana provides that if damage resulting from unauthorized access is greater than $500 then the punishment is a fine not over

325. WYO. STAT. § 6-3-501 to -505 (1983).
326. *Id.* § 6-3-502.
327. *Id.* § 6-3-503.
328. *Id.* § 6-3-504.
329. *Id.* § 6-3-409.
330. *Id.* § 37-12-124 (1977).
331. *Id.* § 14-2-203 (1978).
332. ARIZ. REV. STAT. ANN. § 13-2316 (1978); CAL. PENAL CODE § 502 (West Supp. 1984); N.D. CENT. CODE § 12.1-06.1-08 (Supp. 1983); R.I. GEN. LAWS 11-52-2 to -4 (Supp. 1984); WYO. STAT. § 6-3-502 to -504 (1983).
333. TENN. CODE ANN. § 39-3-1404 (Supp. 1984).

$10,000 or imprisonment of not more than five years (at hard labor), or both;[334] and Georgia provides that unauthorized access may be punishable by a fine not exceeding $50,000 or imprisonment not to exceed fifteen years, or both.[335]

Most states which have computer-related statutes, however, tailor their penalty provisions to the various elements of the offense. It is therefore recommended that each particular state penalty provision be reviewed in order to fully appreciate the potential ramifications a violation may hold in a particular state.

V. STATE COMPUTER CRIME VENUE PROVISIONS

Most of the applicable state statutory venue sections provide that prosecution may be brought in the county in which the alleged crime took place or the county where the computer system owned by the victim is located.[336]

VI. STATE ACCOMPLICE PROVISIONS

The question of whether a BBS SYSOP can be held liable for the use (or abuse) of information posted on his/her board tends to fall into the category of conspiracy. There are exceptions, specifically where states have passed laws prohibiting the publishing of telephone credit codes and the transfer of instructions or specifications for the manufacture of telecommunications theft devices.[337]

In most states, conspiracy is defined as an agreement by two or more persons to commit a crime, where the crime is committed by at least one of the persons based upon that agreement.[338] The question is then directed to whether a SYSOP agrees with another that information posted on the BBS will be used to commit a crime. There is, arguably, a tacit understanding that the information may potentially be used by someone to commit a crime. The question is whether this understanding constitutes an agreement by both parties that at least one of them will commit a crime. Conspiracy provisions must be examined to appreciate how they may be applicable to particular BBS activities in a specific state, since a few states provide additional qualifying provisions. Some states provide for additional penalties under

334. Act of July 13, 1984, § 1, 1984 LA. SESS. LAW. SERV. 711 (West) (to be codified at LA. REV. STAT. §§ 14:73.1 - :73.5).

335. GA. CODE ANN. § 16-9-93 (1984).

336. *See e.g.*, DEL. CODE ANN. tit. 11, § 2738 (1984).

337. *See, e.g.* ARIZ. REV. STAT. ANN. § 13-1307 (1978).

338. *See, e.g.*, DEL. CODE ANN. tit. 11, § 511-13 (1979).

their accessory statutes for the involvement of a juvenile.[339]

VII. APPLICATION OF RELEVANT STATE STATUTES TO BBS ACTIVITIES

To date, there has been only one known arrest of a BBS SYSOP based solely upon information posted on a board. In May of 1984 Mr. Tcimpidis, a Los Angeles, California resident, was arrested[340] and charged under California's statute pertaining to the publishing of telephone credit codes.[341] It is alleged that a stolen telephone credit code was posted on Mr. Tcimpidis' BBS.[342] Mr. Tcimpidis has not yet been tried.[343]

Many personal computer owners and BBS SYSOPs contend that holding a SYSOP liable for the information posted on their BBS violates the First Amendment. Many SYSOPs (especially the younger ones) argue that they have a First Amendment right to free speech under which they can freely post any information.[344] It is the person who goes out and uses that information in a fraudulent manner, they argue, that is the one committing the crime. An analogy to a bulletin board located in a neighborhood supermarket has been attempted.[345] The police will not hold the supermarket liable (and therefore close it down) because one person posts a message to sell a stolen car. SYSOPs then ask why a BBS should be closed down because of one message containing a stolen telephone credit card. This analogy can easily be distinguished. Certainly a SYSOP who does not permit the posting of hacker or phreaker information, and makes reasonable efforts to prevent such information from being posted, will have a defense under a related prosecution. There are a large number of BBSs, however, which cater to, and encourage, the posting of hacker and phreaker information.[346] Under the above analogy, if a neighborhood establishment (even a supermarket) openly permitted and encouraged messages relating to stolen goods to be posted on its public bulletin

339. *See, e.g.*, IDAHO CODE § 18-204 (1979).

340. *See* Stipp, *Computer Bulletin Boards Fret Over Liability for Stolen Data*, Wall St. J. Nov. 9, 1984, at 33, col. 1.

341. CAL. PENAL CODE § 502.7 (West Supp. 1984).

342. Stipp, *supra* note 340, at 33, col. 1.

343. Since the completion of this article, the authors have been advised that the charges against Mr. Tcimpidis have been dropped. Because the Tcimpidis case raises significant constitutional issues, the authors decided not to delete its discussion. *See infra* text accompanying notes 344-48.

344. Stipp, *supra* note 340, at 33, col. 1.

345. *Id.*

346. *Id.*

boards, one would expect the local authorities to remove the element facilitating the crime—the bulletin board—and not shut down the establishment.

What is most significant in Mr. Tcimpidis' case is that he asserts that his BBS was not a hacker or phreaker board, but completely legitimate.[347] The illegal information was posted, he contends, while he was out of town.[348] If Mr. Tcimpidis was indeed running a legitimate BBS and he is still convicted, then many of the First Amendment arguments immediately become more viable. Virtually anyone can call a BBS and leave a message. The issue is whether a SYSOP is automatically liable for any potentially criminal messages posted on his/her board. A second concern is whether a SYSOP is expected to continuously monitor his/her BBS and immediately remove any suspect messages.

Similar First Amendment arguments were raised in the case of *State v. Northwest Passage, Inc.*[349] which involved the newspaper publication, in violation of a state statute, of information disclosing the method then used by AT&T to establish credit card numbers.[350] The Supreme Court of Washington held that the statute did not substantially restrict protected speech when judged in relation to the statute's legitimate function of preventing fraud.[351]

VIII. FEDERAL COMPUTER CRIME LAWS

The United States Congress has been concerned with the threat of computer crimes. This is evidenced by the number of computer-related bills which have been introduced in the past few years. Following are listed recently proposed bills.

The Senate had three major computer crime bills pending. S. 1733 would have made the fraudulent or illegal use of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce, a crime.[352] S. 1920 would establish a Small Business Computer Crime and Security Task Force.[353] S. 2270 would have also made the fraudulent or illegal use of any computer owned or operated by the United States, certain fi-

347. *Id.*
348. *Id.*
349. 17 Wash. App. 685, 564 P.2d 1188 (1977), *rev'd*, 90 Wash. 2d 741, 585 P.2d 794 (1978).
350. *Id.* at 686-87, 564 P.2d at 1189.
351. State v. Northwest Passage, 90 Wash. 2d 741, 585 P.2d 794 (1978).
352. S. 1733, 98th Cong., 2d Sess. (1984).
353. S. 1920, 98th Cong., 2d Sess. (1984).

nancial institutions, and entities affecting interstate commerce, a crime.[354] The bill would also have punished anyone who damages, destroys, alters, or deletes any computer program or computer-stored information intentionally and without authorization.[355] In addition, S. 2270 would have made it unlawful to intentionally buy or sell a password or access code to a computer for the purpose of executing a scheme to defraud or to obtain money, property, or services.[356]

As of fall 1984, there were eight bills pending in the House of Representatives which related to the specific activities covered in this article. HR. 1092 provided for: (1) using, or attempting to use, an applicable computer with intent to execute a scheme or artifice to defraud, or to obtain property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or knowingly convert to one's own use or the use of another, the property of another; or (2) intentionally and without authorization damaging an applicable computer, or causing, or attempting to cause, the withholding or denial of the use of a computer, a computer program or stored information. Under this bill, an applicable computer must be owned by, be under contract to, or be operated on behalf of the United States Government, or a financial institution involved in interstate commerce.[357]

HR. 3181 provided for the unauthorized transfer of a fraudulent payment device. Under the bill, a fraudulent payment device was defined, inter alia, as a code or account number used to obtain goods or services, which had been stolen or fraudulently obtained.[358] HR. 4259 included provisions for: (1) the willful use, attempted use, or unauthorized access of a qualified computer with intent (a) to execute a scheme or artifice to defraud, or obtain property by false or fraudulent pretenses, representations, or promises; (b) to embezzle or steal property; or (c) to use the property of another; and (2) intentionally and without authorizations (a) damaging a qualified computer; or (b) causing or attempting to cause the withholding or denial of the use of a qualified computer, or a computer program or stored information relating to a qualified computer. The bill defined a qualified computer as a computer that operated in, or used a facility of, interstate commerce.[359]

HR. 4301 made the unauthorized use of a computer which affects

354. S. 2270, 98th Cong., 2d Sess. (1984).
355. *Id.*
356. *Id.*
357. H.R. 1092, 98th Cong., 2d Sess. (1984).
358. H.R. 3181, 98th Cong., 2d Sess. (1984).
359. H.R. 4259, 98th Cong., 2d Sess. (1984).

interstate or foreign commerce, a crime.[360] HR. 4384 was essentially identical to HR. 4259.[361] HR. 4954 provided penalties for the use of a telecommunications device to obtain unauthorized direct access to a medical record.[362] HR. 5112 provided for knowingly, and without authorization, transferring a fraudulent access device.[363] A fraudulent access device was defined under the bill as, inter alia, any code or account number which is used for obtaining goods or services which has been stolen or fraudulently obtained.[364] In addition, HR. 5112 provided for: (1) knowingly, and without authorization, accessing a computer with the intent to execute a scheme to defraud; or (2) knowingly accessing a computer without authorization, and by means of such conduct, knowingly using, modifying, or disclosing information in, or preventing authorized use of, such computer. The above activities must have affected interstate or foreign commerce.[365]

HR. 5616 provided for knowingly, and with intent to defraud, producing or trafficking in one or more counterfeit access devices.[366] Under the bill, "traffic" and "produce" meant, inter alia, to transfer and to duplicate, respectively.[367] HR. 5616 defined access device as including any code or account number used to obtain goods or services.[368] The bill also essentially provided for the knowing and unauthorized access of a computer with the intent to defraud or to use, modify, destroy, or disclose information in, or to prevent the unauthorized use of, a computer operated by or on behalf of the United States Government.[369]

IX. CURRENTLY APPLICABLE FEDERAL LAW

Previously, federal prosecutions which have involved computer fraud utilized the Wire Fraud Act.[370] An example of this application

360. H.R. 4301, 98th Cong., 2d Sess. (1984).
361. H.R. 4384, 98th Cong., 2d Sess. (1984).
362. H.R. 4954, 98th Cong., 2d Sess. (1984).
363. H.R. 5112, 98th Cong., 2d Sess. (1984).
364. *Id.*
365. *Id.*
366. H.R. 5616, 98th Cong., 2d Sess. (1984).
367. *Id.*
368. *Id.*
369. *Id. See generally* COMPUTER CRIME L. REP., *supra* note 42.
370. 18 U.S.C. § 1343 (1982). The section provides:

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 a

can be found in the case of *U.S. v. Seidlitz*[371] which involved the unauthorized access of a computer to obtain software stored within the accessed computer.[372] The Wire Fraud Act is also used for blue box prosecutions.[373]

There is now a federal computer-related statute which is cited as the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984."[374] It prohibits the unauthorized access of a computer to: (1) obtain government information considered to be protected for national defense reasons or is restricted;[375] (2) obtain information contained in a financial record of a financial institution or consumer reporting agency;[376] or (3) knowingly use, modify, destroy, or disclose information in, or prevent authorized use of, a computer operated for or on behalf of the United States Government.[377] The maximum penalty under the Act is $10,000 or twice the value obtained by the offense or imprisonment for not more than ten years or both.[378] Furthermore, the Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.[379]

A seven count indictment was handed down by the U.S. District Court for the District of Colorado on February 5, 1985.[380] The indictment alleged violations of 18 U.S.C. Sections 1030, 1343, and 1001. Specifically, a California resident was charged with the unauthorized access of computers in the Denver Regional Office of the Department of Agriculture—Forest Service and the Supervisor's Office of the Arapaho and Roosevelt National Forests in Fort Collins, Colorado. It is further alleged that the defendant had information from the computers transmitted to him and printed out by him. These were the

---

scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both.

Id.

371. 589 F.2d 152 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979).

372. *Id.* at 153.

373. See Annot., 78 A.L.R.3d 449 (1977) for a discussion of criminal prosecutions for the use of "blue boxes." *See also supra* note 6 and accompanying text.

374. Pub. L. No. 98-473, 1981 U.S. CODE CONG., & AD. NEWS. (98 Stat.) 2190 (to be codified at 18 U.S.C. § 1030).

375. *Id.* (to be codified at 18 U.S.C. § 1030(a)(1)).

376. *Id.* at 2190-91 (to be codified at 18 U.S.C. § 1030(a)(2)).

377. *Id.* at 2191 (to be codified at 18 U.S.C. § 1030(a)(3)).

378. *Id.* (to be codified at 18 U.S.C. § 1030(c)).

379. *Id.* at 2192 (to be codified at 18 U.S.C. § 1030(d)).

380. United States v. Fadriquela, No. 85-CR-40, U.S. Dist. Ct. (D. Colo. 1985). In May, 1985, Mr. Fadriquela pleaded guilty to misdemeanor charges under the Act. On June 14, 1985, Mr. Fadriquela was placed on probation and fined $3,000.

alleged 18 U.S.C. section 1030 violations. The alleged 18 U.S.C. section 1343 violations occurred through the unauthorized use of GTE Telenet Communications and Tymnet systems. The alleged 18 U.S.C. section 1001 violations involved the Defendant's misrepresentation that he was an authorized user of the computer systems involved.

X. CONCLUSION

The enacted state statutes[381] and proposed federal computer-related statutes[382] contain a number of common elements. They all generally address the unauthorized access, alteration, damage, and destruction of computer systems and computer programs. The optimal computer-related state and federal statutes would address the following factors: banking/financial transaction devices; telecommunications; and "non-financial" computer systems. An additional essential element is close coordination between federal and state computer statutes.

Banking and financial computers present an attractive target simply because of the enormous daily cash flow. These systems suffer indirect attack through the unauthorized use of financial transaction device codes and account numbers. Optimal federal and state statutes would prohibit the unauthorized use or publication of access codes, methods of creating access codes, and account numbers. The majority of states have statutes which prohibit the manufacture or use of telecommunications theft devices (as well as the sale or transfer of plans or instructions for making the same). The optimal statute would prohibit the manufacture, use, possession, sale, or transfer of these devices, as well as prohibit the possession, sale, transfer, or publication of plans, specifications, or instructions for making these devices. Finally, state and federal statutes must be tailored to the problem of unauthorized computer access alone. Ideally, these statutes would provide that a computer owner, lessor, or operator must provide notice that unauthorized access, or attempted unauthorized access, would be a violation of applicable state or federal statutes.

Application of state or federal statutory provisions should be relatively identical. The only exceptions would apply to jurisdictional and juvenile considerations. State computer-related statutes would apply to computers located within the state boundaries, whereas the federal statutes would include all computers involved in interstate commerce

381. *See supra* notes 18-327 and accompanying text.

382. *See supra* notes 348-365 and accompanying text.

(in effect, all computers owned by major corporations) and all computers owned, operated, or leased by the United States government.

Juvenile law considerations are paramount to an optimal computer-related statute given that a large number (if not a majority) of hackers are under eighteen years of age. Federal statutes could either defer to the juvenile laws of the state holding ancillary jurisdiction or contain a complete federal juvenile computer statute. State laws should make specific provisions for this new type of "white collar crime" by providing educational, community service, and some type of temporary impounding of computer hardware and software penalties in juvenile adjudications. In addition, parental liability statutes should be amended to reflect more accurately the potential monetary damage of which a juvenile hacker is capable.

An essential element to any optimal computer-related federal and state statutory scheme is education. As a preventative measure, young computer enthusiasts must be taught a computer ethic which includes acknowledgment that computer data is private property and computer systems are not playgrounds to test computer-logic skills. Parents must also be enlightened to the fact that their children staying home and hacking into computer systems is a serious matter and could cause extensive damage. Prosecutors and judges must also be educated so that they better understand the ramifications of these computer activities.

APPENDIX A

SAMPLE COMPUTER BULLETIN BOARD

NAME ->
FROM ->DENVER, CO
LAST ON ->07/31/84
YOU ARE CALLER #6824

BASE NEWS (9-9-84)

WHY WAS THE SYSTEM DOWN? WELL I LOST A WHOLE DRIVE FULL OF FILES FROM EITHER A DISK ERROR OR A BAD SECTOR. I HAVE BEEN TRYING ALL THIS WEEK TO RECOVER IT TO NO AVAIL. WHAT WAS LOST? THE PIRATE AND THE MAIN BOARDS.

PROBLEM: IT SHOULD NOT HAVE TAKEN ME SO LONG TO GET THE BOARD UP AGAIN. IT IS JUST THAT SCHOOL TAKES SO MUCH TIME (I GET HOME AROUND 6:00 WITH 3-4 HRS. OF HOMEWORK.). SO I AM THINKING OF SELLING THE BOARD, MAYBE JUST THE SOFTWARE, MAYBE SOME ACCESSORIES (CLOCK ETC.), OR MAYBE THE WHOLE SYSTEM. PLEASE LEAVE ME MAIL IF YOU ARE INTERESTED IN PURCHASING ANYTHING AND WE CAN DISCUSS PRICE ETC.

UNTIL THE SYSTEM IS SOLD I WILL TRY TO KEEP IT RUNNING AS BEST I CAN.

WELCOME TO THE BOARD

TODAY IS 09/13/24

SYSOP ->

BULLETINS FROM 1 TO 2
THERE ARE NEW BULLETINS
NO MAIL WAITING

COMMAND (?=HELP):?

CTRL-S STOP/START CTRL-X TO EXIT

file #8493-5344d
General menu. Security level one.

B-go to the message center
P-GO TO THE PIRATE BOARD
BAR-GO TO THE CONVERSATION BAR
TELCO-TELECOMMUNICATIONS SECTION
AE-GO TO THE AE INFORMATION SECTION
D-download information
H-get help
E-examine your dossier
F-send a message to the base commander
R-read intra-base communications

S-send intra-base communications
V-change video width
I-information about system
$-base news
C-call base commander
N-nulls
T-discontinue session
G-general informational files
Z-make phone number (in)visible

end of file.

COMMAND (?=HELP):TELCO

TELCO COMMAND (?=HELP):?

CTRL-S STOP/START CTRL-X TO EXIST

TELECOMMUNICATIONS MENU#122349981
SECURITY LEVEL 1

B-GOTO TELCO BULLITEN BOARD
G-LOOK AT TELCO FILES
A-ABORT BACK TO MAIN MENU

TELCO COMMAND (?=HELP):B

BULLETINS FROM 1 TO 84

OPTION (?=HELP):N

NEW BULLETINS

CTRL-S STOP/START CTRL-X TO EXIT
CTRL-N FOR NEXT BULLETIN

NUMB ->37
SUB ->!!! H E L P !!!
FROM ->SUN LION (#20)
DATE ->08/01/84 15:36:14

SORRY TO INTERRUPT, BUT IS THIS A THREE PERSON BOARD?????
SERIOUSLY THO-
DOES ANYONE KNOW ANY #'S FOR AIRLINE SCHEDULES AND RATES (& MAYBE DIRECT ME TO AUTO-RESERVATION SYSTEMS)????????

THANKS, ++SUN LION++

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->38
SUB ->1500 ft. remote phone

FROM ->NESSUS SHIRTMAKER (#133)
DATE ->08/03/84 22:39:22

For those of you interested, DAK INCORPORATED is selling a phone that supposedly exceeds the FCC limit alotted to cordless phones. This cordless has 1500' range, twice that of most of the better ones, and it's selling via mail order or toll free credit card order for about $110. If you're interested in using this to keep the FBI running in circles, leave me E-MAIL or just express you're interest here, and I'll post the toll-free order number, the adress, and exact price of this phone.

Leighter Deighze,
Nessus Shirtmaker

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->39
SUB ->12 MILE RADIUS
FROM ->SYSOP
DATE ->08/04/84 15:08:57

IN JAPAN THEY HAVE THESE CORDLESS PHONES THAT HAVE 12-30 MILE RANGE! THE UNIT IS CONTAINED IN A BREIFCASE WITH A SCRAMBLER (LIKE THE BOND FLICKS). TOO BAD THE FCC WOULD BITCH ABOUT IT.

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

SUB ->Here it is...
FROM ->NESSUS SHIRTMAKER (#133)
DATE ->08/04/84 18:51:35

Okay D.M. and all the rest of you, here is the order info on the DAK cordless.

Toll free credit card orders; call 1-800-325-0800
24 Hours a day, 7 days a week.

Mail order (sorry, no COD's)

mail to DAK INDUSTRIES INC.
10845 Vanowen ST.
N. Hollywood, CA 91605

There it is. I'm not a sales rep. or anything. I just got a catalog in the mail, and it has a lot of neat-o stuff in it.

If you have anymore questions, leave E-mail to me.

Leighter Deighze,
Nessus Shirtmaker

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->41
SUB ->cont from above
FROM ->NESSUS SHIRTMAKER (#133)

DATE ->08/04/84 19:03:32

O crud. I forgot to mention some more.
Here are the order numbers to use when you mail in or call

Cordless with10 stored # capability; order #9738 and it's $109 + $4 P&H

Cordless with nonmemory capability; order #9739 and it's $99 + $4 P&H

Notes to inquirers;
It uses universal pulse dialing that is compatible with both rorary & Touch-Tone.

Adios
Nessus Shirtmaker

PS
Tomarrow (or soon) I'll post info on an incredible printer.

One of the many incredible products brought to your attention by the scryings of Nessus Shirtmaker & Company.

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->42
SUB ->THE LAND
FROM ->THE PSUEDONYM (#12)
DATE ->08/04/84 23:39:16

```
* ********************************************************************** *
*                                CALL...                                 *
*                                                                        *
*                          <*> THE LAND <*>                              *
*                                                                        *
*                                                                        *
*                            300/1200 BAUD                               *
*                                                                        *
* ---------------------------------------------------------------------- *
*((((((((((((((((((((((((((((((((SYSTEM    HOURS))))))))))))))))))))))))))))))*
*                                                                        *
* MON-FRI 5PM TO 10 PM                                                   *
* SAT-12 PM TO 6PM                                                       *
* SUN-12PM TO 10PM                                                       *
*                                                                        *
* ---------------------------------------------------------------------- *
*----------------------------------SPECIAL    NOTE----------------------*
* To Log Onto the System At 300                                          *
* Baud You Need to Press The                                             *
* Return Key Until It Comes Up                                           *
* Onto the Screen...The 1200                                             *
* Baud Is Inactive(System Bo-Bo)                                         *
* Should Be Able to Support It By                                        *
```

```
* Wendsday (Darn!)...Ask For Phreak                                    *
* Access.....New Board...Needs Mes-                                    *
* sages....Soon To Come On The Board                                   *
* An Ae-Line....Must Get Hard Disk                                     *
* Working!!!!                                                          *
* ******************************************************************** *
********************** CALL TODAY! **********************
* ******************************************************************** *
```

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->44
SUB ->NEED CORLESS!
FROM ->DAN MACMILLAN (#78)
DATE ->08/06/84 11:41:11

HIGH! I AM IN DIRE NEED OF A CORDLESS FONE THAT WILL DILE WITH *TONE*, A MEMORY WOULD BE NICE, AND I'D LIKE TO GET IT WITH A CREDIT CARD....
IF ANYONE CAN RECOMMEND ONE PLEASE DO SO!
THANX
DAN MACMILLAN

NUMB ->45
SUB ->MODEM
FROM ->THE LODE RUNNER (#414)
DATE ->08/06/84 15:09:42

First of all, to The Chip, great idea! Why don't we just drop the bar o delete all the old bulletins off of it to make more disk space? Also:

Modem for sale!!!!

Era 2 modem
plug-in card for the apple
Hayes Smartmodem compatable
300/1200 baud
auto-dial/answer
and more...

All this for only:

$225

For more info or if you are interested in buying this please leave me mail.

—> The Lode Runner
(#414)

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->46
SUB ->IT'S NOT THAT
FROM ->THE TREKKER (#489)

DATE ->08/08/84 23:05:34

IT'S NOT THAT WE SHOULD TAKE OFF THE BA R(SOOR
SORRY) IT IS THAT PAUL AND THE OTHERR GUYS WHO STILL HAVE OLD MESSAGES, THEY SHOULD DELETE THEM! I CAN'T EVEN READ MY E-MAIL WITHOUT GETTING OOPS SYSTEM ERROR!

THE TREKKER

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->47
SUB ->NUMBERS
FROM ->KILROY WAS HERE (#33)
DATE ->08/09/84 12:43:33

MCI MAIL:303-831-8139
USER ID:TSPAND
PSWD:DOHIJAVO

METRO:623-5326
181064 228057 228367 228337 228110

JEFCO COMP.:278-6001

THAT'S ALL FOR NOW.

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->48
SUB ->Y
FROM ->THE CHIP (#405)
DATE ->08/10/84 00:11:54

UNIX BASED SYSTEMS:
202-636-3469
1-800 EXTENDERS:
1-800-328-1470
666666
640
METROS:
228337
228367
181064
228057
228113
CONF:
213-080-1050
213-080-3050
THE CHIP
PS: ANDY BODY KNOW OF ANY COSMOS SYSTEM AND PASWORDS?

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->49
SUB ->cosmos
FROM ->BROADWAY HACKER (#157)
DATE ->08/11/84 12:43:17

I have plenty of Cosmos p/ws and dialups, and wirecenters (if you know what those are).

What kind of idiot tries dialing a conference number on a phone!!!

What area did you need cosmos for, Chip?

*** Broadway Hacker ***

NYCity Summer Hackattack '84
<-=CENTRAL-DATA=->

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->50
SUB ->CONFERENCING WITH 2600Hz
FROM ->THE CHIP (#405)
DATE ->08/11/84 14:49:22

=-=-=-=-=-=-=-=-=-=-=-=-=

STARTING A CONFERENCE

TO DO THIS YOU NEED EITHER A BLUE BOX OR AN APPLE CAT AND A BLUE BOX ' PROGRAM LIKE "THE CAT'S MEOW"

1. DIAL OUT TO A TOLL FREE DIRECTORY SERVICE NUMBER LIKE 1-514-555-1212

2. BEFORE THE OPERATOR ANSWERS, HIT AND KEEP PUSH 2600hz UNTIL SHE DOES THIS SHOULD THROW YOU INTO A MAIN TRUNK LINE ONLY USED BY THE OPERATORS CONSOLE.

3. NOW CHANGE FROM TOUCH-TONE (TM) TO MULTI-FREQUENCY (MF) AND DIAL THE FOLLOWING:
   'KP+213+080+105'X'+ST'
   WHERE 'X' IS ANY NUMBER FROM 1 to 6. DO NOT TRY TO DAIL THE QUOTE MARKS OR THE X.
   EXAMPLE:
   KP+213+080+1051

4. AFTER HITTING ST, YOU WILL HEAR A CHIRP. THEN DIAL THE BILLING NUMBER. IT IS BEST TO USE THE FOLLOWING:
   KP+213+080+1050
   THIS IS SO NO ONE GET'S BILLED.

5. WHEN THE RECORDING ASKS YOU FOR THE NUMBER OF LINES, USE A NUMBER IN THE AREA OF 20 TO 30. YOU CAN

HAVE FROM 1 to 50 BUT IF THEY DONT HAVE 50 LINES, THEY TELL YOU TO CALL BACK.

CONT....

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->51
SUB ->CONFERENCING WITH 2600HZ
FROM ->THE CHIP (#405)
DATE ->08/11/84 14:51:26

6. THIS CONF. NUMBER IS OPEN BETWEEN 7:AM to 5:PM CALIFORNIA TIME. IT IS BEST TO GET A UNUSED LOOP NUMBER AND TRANSFER CONTROL TO ONE END EARLY IN THE MORNING. THAT WAY YOU CAN'T BE TRACED AND YOU DONT HAVE TO WORRY ABOUT GETTING ONE GOING AROUND FOUR OR SO WHEN THEY ARE ALL BUSY. JUST HOOK UP TO IT AROUND 8 OR 9 AM AND LEAVE IT. THEN CALL THE OTHER END OF THE LOOP WHEN YOU WANT IT BACK.

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->52
SUB ->CONFERENCE CONTROL
FROM ->THE CHIP (#405)
DATE ->08/11/84 14:54:07

=-=-=-=-=-=-=-=-=-=-=
CONFERENCE INFO
=-=-=-=-=-=-=-=-=-=-=

CONFERENCE CONTROL
==========
ONCE YOU HAVE CONTROL, YOU CAN PUNCH THE # KEY ON YOUR PHONE AND YOU WILL HAVE CONTROL. USE THE FOLLOWING:

: BRINGS YOU OUT OF THE CONFERENCE AND INTO CONTROL MODE.

: ALSO BRINGS YOU AND THE PARTY (OR NO PARTY IF YOU WANT) BACK INTO THE CONFERENCE.

* : BACKS UP ONE STEP IF YOU MADE A MISTAKE OR HANGS UP THE LINE YOU CALLED WHEN IN CONTROL MODE.

1 : WHEN IN CONTROL MODE, AND YOU WANT TO SEE IF SOMEONE IS HOME TO BE ADDED TO THE CONF, DIAL 1+THE AREA CODE+ THE NUMBER, JUST LIKE MA-BELL.

7 : BLOWS THE CONFERENCE LINE, HANGS UP.

6 : TRANSFERS CONTROL TO ANOTHER NUMBER OR ONE SIDE OF A LOOP.

9 : SILENT ATTENDANT.

CONT...

[A]UTO REPLY [N]EXT [R]E-READ [Q]UIT :N

NUMB ->53
SUB ->CONFERENCE CONTROL
FROM ->THE CHIP (#405)
DATE ->08/11/84 15:04:24

HINTS:
======

ONE OFTEN THING THAT CONFERENCES ARE USED FOR ARE MINNI TELE-TRIALS. THIS IS WHEN SOME ASS HOLE HAS DONT SOMTHING AND EVERYONE ON THE CONF. WANTS TO CALL HIM UP AND RAG ON HIM. THE PROBLEM IS, ONCE YOU HAVE SENT HIM INTO THE CONFERENCE, YOU HAVE NO OVER HIM, AND YOU CANOT BLOW HIM OFF. THE WAY TO FIX THIS IS TO FIRST, GO INTO CONTROL MODE, THEN CALL UP MCI OR SPRINT. GET THE TONE, INPUT THE CODE AND CALL THIS PERSON, THEN PUT THEM ON THE CONFERENCE. IF THEY START PLAYING MUSIC OVER THE LINE OR PUNCHING BUTTONS, JUST BLOW A LOUD 2600hz TONE AND MCI OR SPRINT WILL HANG THEM UP. NEET HA!

ANOTHER INTERRESTING THING THAT CAN BE DONE IS THIS:
MANY PHREAKS LIKE TO GET OPERATORS ON THE LINE TO GET INFO OUT OF THEM OR THEY LIKE TO BRING ON HUNDREDS OF OPERATORS AND SCREW THEM UP ALL AT THE SAME TIME. WHEN BRINGING ON HUNDREDS, THE BEST THING TO DO IS THIS. DIAL UP ABOUT 20 OR THIRTY DIRECTORY SERVICE PEOPLE ONTO THE CONF. KEEP THEM BUSY AND IMPERSONATE A TSPS OR SUPERVISOR OR SOMETHING. WHEN THEY START HANGING UP, THE CONF CONTROL HAS AN AUTOMATIC REDIAL WITH THE PUNCH OF THE # BUTTON. YOU CAN JUST KEEP CALLING THEM BACK UP. IF IT IS A CO OR "O" OPERATOR, IT IS SUGGESTED THAT YOU USE A LOOP CONFERENCE AND AN EXTENDER CAUSE THEY CAN TRACE. 1-800 NUMBERS CANNOT BE BROGHT ON A CONF BUT YOU CAN IF SOMEONE USES THREE-WAY. THE MOST IMPORTANT THING TO DO IS TIE UP THE LINE BEFORE CALLING AN OPERATOR. RUN IT THROUGH A FEW CITIES FIRST.
HAVE FUN.....!
THE CHIP

APPENDIX B

COMPUTER CRIME STATUTES (ANALYSIS BY STATE)

	In General	Fraud Provision	Data Destruct.	Equipment Destruct.	Access Only	Other Provision
ALABAMA						X
ALASKA	X	X	X			X
ARIZONA	X	X	X	X	X	
ARKANSAS						
CALIFORNIA	X	X	X	X	X	
COLORADO	X	X	X	X	X*	
CONNECTICUT	X	X**	X	X	X	
DELAWARE	X	X	X	X	X	
D.C.						
FLORIDA	X	X	X	X	X	
GEORGIA	X	X	X	X	X	
HAWAII	X	X	X	X	X	
IDAHO	X	X	X	X	X	
ILLINOIS	X	X	X	X	X**	
INDIANA						
IOWA	X	X	X	X	X	
KANSAS						
KENTUCKY	X	X	X	X	X	
LOUISIANA	X	X	X	X	X	
MAINE						X
MARYLAND	X				X	X
MASSACHUSETTS						X

* Statutes prohibits unauthorized use. ("Use" is defined similarly to most states' definition of "access").

** Statute only refers to unauthorized use.

	In General	Fraud Provision	Data Destruct.	Equipment Destruct.	Access Only	Other Provision
MICHIGAN	X	X	X	X	X	
MINNESOTA	X	X	X	X		
MISSISSIPPI						
MISSOURI	X	X	X	X	X	
MONTANA	X	X**	X	X	X**	
NEBRASKA						
NEVADA	X	X	X	X	X	
NEW HAMPSHIRE						
NEW JERSEY						
NEW MEXICO	X	X	X	X	X	
NEW YORK						
NORTH CAROLINA	X	X	X	X	X	
NORTH DAKOTA	X	X	X	X	X	
OHIO						X***
OKLAHOMA	X	X	X	X	X	
OREGON						
PENNSYLVANIA	X	X	X	X	X	
RHODE ISLAND	X	X	X	X	X	
SOUTH CAROLINA	X	X	X	X	X	
SOUTH DAKOTA	X	X	X	X	X*	
TENNESSEE	X	X	X	X	X	
TEXAS						
UTAH	X	X	X	X		

** Statute only refers to unauthorized use.

*** Definitions under Theft provisions include sections relating to computers, but no other specific language.

	In General	Fraud Provision	Data Destruct.	Equipment Destruct.	Access Only	Other Provision
VERMONT						
VIRGINIA	X	X	X	X†		
WASHINGTON	X		X	X††	X††	
WEST VIRGINIA						
WISCONSIN	X	X	X	X	X	
WYOMING	X	X	X	X	X	
TOTAL	34	32	33	32	30	6

† Statute refers to the "physical injury to the property of another."
†† Statute relates to "Computer Trespass."

APPENDIX C

TELECOMMUNICATIONS FRAUD STATUTES (ANALYSIS BY STATE)

	Telcomm. Fraud In General	Telcomm. Fraud by Device	Publishing of C.C. Codes	Telcomm. Theft of Services
ALABAMA	X	X		
ALASKA				
ARIZONA	X	X	X*	
ARKANSAS				
CALIFORNIA	X	X	X	
COLORADO		X		
CONNECTICUT				X
DELAWARE		X	X†	
D.C.				X
FLORIDA	X	X	X	
GEORGIA	X	X	X	
HAWAII		X		X
IDAHO	X	X	X	
ILLINOIS	X	X	X	
INDIANA		X		X
IOWA				
KANSAS	X**	X	X	
KENTUCKY		X		
LOUISIANA	X	X		
MAINE		X		X
MARYLAND		X	X	X

* Statute prohibits disclosure of codes.

** Kansas has separate statutes pertaining to both civil and criminal sanctions.

† Statute pertains to the publishing of credit codes in general (not specifically related to telephone credit card codes).

	Telcomm. Fraud In General	Telcomm. Fraud by Device	Publishing of C.C. Codes	Telcomm. Theft of Services
MASSACHUSETTS	X	X	X	
MICHIGAN	X	X		
MINNESOTA	X	X		
MISSISSIPPI	X	X		
MISSOURI				
MONTANA	X	X	X	
NEBRASKA		X		X
NEVADA	X	X		
NEW HAMPSHIRE		X	X*	X
NEW JERSEY		X		X
NEW MEXICO	X	X		
NEW YORK		X		X
NORTH CAROLINA	X	X	X	
NORTH DAKOTA		X	X	
OHIO	X	X		
OKLAHOMA	X	X	X	
OREGON		X		X
PENNSYLVANIA		X	X†	
RHODE ISLAND		X	X	
SOUTH CAROLINA	X	X		
SOUTH DAKOTA	X	X		
TENNESSEE	X	X		
TEXAS		X	X	

* Statute prohibits disclosure of codes.

† Statute pertains to the publishing of credit card codes in general (not specifically related to telephone credit card codes).

	Telcomm. Fraud In General	Telcomm. Fraud by Device	Publishing of C.C. Codes	Telcomm. Theft of Services
UTAH		X		
VERMONT	X			
VIRGINIA	X	X		
WASHINGTON	X	X	X	
WEST VIRGINIA	X	X		
WISCONSIN	X			
WYOMING	X	X		
TOTAL	28	43	19	11