Richmond Journal of Law and Technology

Volume 7 | Issue 3 Article 4

2001

State Cybercrime Legislation in the United States of America: A Survey

Susan W. Brenner

Volume VII, Issue 3,

Winter 2001

State Cybercrime Legislation in the United States of America: A Survey

by: Susan W. Brenner(*)

Cite As: Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J.L. & TECH. 28 (Winter 2001), *at* http://www.richmond.edu/jolt/v7i3/article2.html.

TABLE OF CONTENTS

I. INTRODUCTION

{1}In the United States, cybercrimes are the focus of legislation adopted at both the state and federal levels. The U.S. Constitution allocates lawmaking authority between the two levels according to certain principles, (1) one of which is that even when federal jurisdiction to legislate exists, federal legislation is appropriate only when federal intervention is required.(2) And while federal legislative authority can pre-empt the states' ability to legislate in a given area, it rarely does, so it is not unusual for federal criminal laws to overlap with state prohibitions that address essentially the same issues.(3)

{2}There are a number of federal statutes which address varieties of cybercrimes.(4) The omnibus federal cybercrime statute is 18 U.S. Code § 1030. This statute makes it an offense to do any of the following to and/or by means of a computer used by a financial institution, by the federal government or used in interstate or foreign commerce or communication:

(a) gain unauthorized entry into a government computer and thereby discover information which is intended to remain confidential, information which the perpetrator either unlawfully discloses to someone not authorized to receive it or retains in violation of the law;

(b) gain unauthorized entry to a computer and thereby gains access to information to which the perpetrator is not entitled to have access;

(c) gain unauthorized access to a computer and thereby furthers the perpetration of a fraud;

(d) cause damage to a computer as the result either of gaining unauthorized access to it or of inserting a program, code or information into the computer; or

(e) transmits, in interstate or foreign commerce, a threat to cause damage to a computer in order to extort money or property from a person or other legal entity.(5)

{3}Section 1462 of title 18 of the U.S. Code prohibits using a computer to import obscene material into the United States, while 18 U.S. Code Section 1463 outlaws using a computer to transport obscene material in interstate or foreign commerce. Section 2251 of title 18 of the U.S. Code makes it a crime to employ a minor in or induce a minor to participate in making a visual depiction of a sexually explicit act if the depiction was created using materials that had been transported (including transportation by computer) in interstate or foreign commerce. Section 2251(A) of title 18 of the U.S. Code prohibits using a computer to sell or transfer custody of a minor knowing the minor will be used to create a visual depiction of sexually explicit conduct. Sections 2252 and 2252(A) of title 18 of the U.S. Code makes it a crime to use a computer to transport child pornography in interstate or foreign commerce.

{4}Another statute - 18 U.S.C. § 1028 - makes it a crime to produce, transfer or possess a device, including a computer, that is intended to be used to falsify identification documents. Finally, 18 U.S.C. § 2319 makes it a federal offense to infringe a valid copyright. Many of the other statutes outlaw "traditional" crimes - such as threatening the President's life - and in so doing, encompass conduct that is committed via a computer.

{5}While some suggest cybercrime legislation and enforcement should be reserved for federal authorities, there is a historical preference for having states play the primary role in criminal law enforcement(6) and they are addressing cybercrimes. This paper surveys legislation the various states have adopted to that end.

II. FRAMEWORK

{6}Each of the fifty states is free to assert its own legislative idiosyncrasies. There is no formal mechanism - at either the state or federal level - which requires or even prods states to adopt uniform, consistent laws. There are model statutes, such as the Restatements, Uniform Acts and the Model Penal Code,(7) that are drafted by private groups and offered to the states as examples, in the hope that states will adopt their provisions and thereby move closer to uniform legislation.(8)

{7}The framework utilized below, based on the Model State Computer Crimes Code,(9) was created by organizing state cybercrime statutes into eight categories: procedural issues; non-sexual crimes against persons; sexual crimes; crimes involving computer intrusions and damage; fraud and theft crimes; forgery crimes; gambling and other crimes against public morality; and crimes against government.

A. *Procedural Issues*

{8}Many states have adopted legislation that targets procedural issues involved in prosecuting cybercrimes. Some have added definitional sections that augment cybercrime-specific statutes and/or general criminal statutes.(10) Others have adopted statutes which set offense levels and penalties for cybercrimes,(11) establish time periods for commencing prosecution of cybercrimes,(12) and address possible defenses to cybercrime charges.(13)

{9}Still others address jurisdiction. It can be difficult to apply traditional jurisdictional predicates-such as committing all or part of a crime within a state(14) or "causing harm" to someone in a state through acts committed outside a state(15) -- to cybercrimes. In an effort to overcome these difficulties, states are devising different standards for cybercrimes. One approach declares that if someone perpetrates a crime by accessing a computer in another state, the offender will be "deemed to have personally accessed the computer" in both states and can be prosecuted in either state.(16) Other states exercise jurisdiction if the "transmission that constitutes the offense" originates in that state or is received in it;(17) Ohio asserts jurisdiction over one who allows "any writing, data [or] image . . . to be disseminated or transmitted into this state in violation of the law of this state."(18) Some cyber-sex-crime laws base jurisdiction on the victim's presence within the prosecuting state and the defendant's awareness of facts which made the victim's presence within that state "a reasonable possibility;"(19) others assert jurisdiction over one who commits "computer pornography" if the offense involved "a child residing in this state, or another person believed by the person to be a child residing in this state."(20)

B. *Non-sexual Crimes Against Persons*

{10}There are relatively few statutes dealing with non-sexual crimes against persons. No state, for example, has a "cyber-homicide" provision, though a few make it an offense to break into or tamper with a computer system and thereby cause the death of one or more persons or create a strong probability of causing death to one or more persons.(21) Virginia makes it an offense to use "a computer or computer network without authority and with the intent to cause physical injury to an individual."(22)

{11}Only about sixteen states outlaw online stalking or harassment, and several of them require that an offender transmit a "credible threat" to injure the victim, the victim's family, or "any other person."(23) Other statutes are broader, making it a crime to use a computer to "engage in a course of conduct" that would cause

a "reasonable person" to "suffer intimidation or serious inconvenience, annoyance or alarm," as well as to fear death or injury to themselves or to members of their family.(24) Some states have expanded their "obscene phone call" statutes so that they encompass using a telephone or an "electronic communication device" to contact someone and threaten to injure that person or his/her family, to use obscene language, or to make repeated contacts in an effort to annoy the person.(25) Earlier this year, a New York court held that a similar provision encompassed harassing or threatening messages sent via the Internet.(26) Bills have been introduced to make online stalking and/or harassment an offense in states where it is not currently outlawed.(27)

C. *Sexual Crimes*

{12}Next to the intrusion offenses discussed in the next section, sexual crimes account for the largest number of state cybercrime statutes. Most of the statutes are concerned with soliciting sex from minors or soliciting child pornography.

{13}A number of states make it a crime to use a computer to solicit or lure a minor to engage in an "unlawful sex act."(28) Since most, if not all, states have generic statutes that make it a crime for an adult to solicit sex from a child,(29) and since these generic solicitation statutes would presumably encompass use of a computer for this purpose, these statutes appear to be redundant. States clearly do not agree, however, because bills have been introduced to add cyber-solicitation statutes to codes which do not already have them.(30) For some reason, one state makes it a more serious offense to use a computer to solicit a child than to do so in person.(31)

{14}Several states make it a crime to use a computer to compile information about a child "for the purpose of facilitating, encouraging, offering or soliciting a prohibited sexual act" from that child.(32) These statutes are part of an effort to outlaw child pornography.(33) Many states prohibit using a computer to create, store and/or distribute child pornography,(34) and many also prohibit using a computer to send obscene material to a child.(35) Pennsylvania makes it an offense to use a computer to communicate with a child for the purpose of engaging in prostitution.(36)

D. *Crimes Involving Intrusion and Damage*

{15}By far the greatest number of state cybercrime statutes are concerned with computer intrusions and damage caused by intrusions. The intrusion statutes fall into two categories: trespass and vandalism statutes. Most states have a trespass ("hacking") statute which makes it a crime to purposely access a computer, computer system or network without authorization.(37) Most states also have a vandalism ("cracking") statute which typically makes it a more serious crime to purposely access a computer without authorization and alter, damage or disrupt the operation of the computer and/or the data it contains.(38) A few states add a "misuse of computer information" statute which prohibits copying, receiving or using information that was obtained by violating a hacking or cracking statute.(39) New York has what is in effect a cyber-burglary statute that makes it a crime to break into a computer or computer system "with an intent to commit or attempt to commit or further the commission of any felony."(40)

{16}A few states outlaw the creation and transmission of viruses and other harmful programs,(41) and bills to this effect have been introduced elsewhere.(42) A handful make it a crime to introduce false information into a computer system for the purpose of "damaging or enhancing" someone's credit rating.(43) A surprising number have created an "offense against computer equipment or supplies," which consists of modifying or destroying "equipment or supplies that are used or intended to be used in a computer, computer system, or computer network".(44) Even more make it a crime to deny, disrupt, degrade, interrupt or cause the denial, disruption, degradation or interruption of computer services or of access to a computer.(45) A few make it a

crime to destroy computer equipment,(46) and North Carolina makes it a crime to threaten to damage a computer or computer system in order "to extort money or any pecuniary advantage, or . . . to compel any person to do or refrain from doing any act against his will".(47)

{17}Several states outlaw "computer invasion of privacy," which consists of using a "computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority".(48) Others make it a crime to disclose someone else's computer password.(49)

E. *Fraud and Theft Crimes*

{18}A substantial number of states outlaw using computers to commit fraud,(50) i.e., using a "computer, computer system, computer network, or any part thereof for the purpose of devising or executing any scheme or artifice to defraud" or for "obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises".(51) States tend to incorporate embezzlement crimes into their computer fraud statutes, rather than creating separate "computer embezzlement" provisions.(52)

{19}A substantial number of states also outlaw "computer theft,"(53) which can encompass any of several discrete offenses: information theft;(54) software theft;(55) computer hardware theft;(56) and theft of computer services.(57) It can also encompass using a computer to commit a theft in a more traditional sense, e.g., to steal property other than data or computer hardware or software.(58) A few states prohibit the unlawful possession of computer data and/or computer software.(59)

{20}Some states have enacted "identity theft" statutes, which make it a crime to "knowingly and with intent to defraud for economic benefit" obtain, possess, transfer, use or attempt "to obtain, possess, transfer or use, one or more identification documents or personal identification number of another person other than that issued lawfully for the use of the possessor."(60) These statutes are not usually phrased as computer crime statutes, but they should qualify as cybercrimes because computers often play an intrinsic role in identity theft offenses.

F. *Forgery Crimes*

{21}A few states outlaw computer forgery, which is defined as follows: "Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery . . . shall be guilty of the crime of computer forgery."(61) At least one state makes it a crime to possess "forgery devices," which include computers, computer equipment and computer software "specially designed or adapted to such use."(62)

G. *Gambling and Other Crimes Against Public Morality*

{22}Only one state has outlawed online gambling: Louisiana created the crime of "gambling by computer," which consists of conducting or assisting in conducting a "game, contest, lottery, or contrivance whereby a person risks the loss of anything of value . . . to realize a profit when accessing the Internet [or] World Wide Web . . . by way of any computer."(63) The Louisiana statute also makes it a crime to develop, maintain or provide computer services, software "or any other product accessing the Internet, World Wide Web, or any part thereof offering to any client for the primary purpose of the conducting as a business of any game . . . whereby a person risks the loss of anything of value in order to realize a profit."(64) Legislation targeting online gambling has been proposed in other states.(65)

{23}At least one state has adopted legislation dealing with purchases of alcoholic beverages via the Internet.

(66) Others have proposed legislation to this effect,(67) and some have proposed legislation which would make it illegal to sell cigarettes via the Internet to citizens of that state.(68)

H. *Crimes Against Government*

{24}Only a few states have make it a crime to use computers to obstruct law enforcement or the provision of government services. Illinois forbid using a computer to cause a "disruption of or interference with vital services or operations of State or local government or a public utility."(69) Several states make it a crime to use a computer to interrupt or impair the delivery of essential services (e.g., services of a public or private utility, medical services, communication services or government services) or to otherwise endanger public safety.(70)

{25}Some states make it a crime to use a computer to obtain information "with the state or any political subdivision which is by statute required to be kept confidential."(71) West Virginia prohibits the unauthorized accessing of information stored in a computer owned by its state legislature.(72) Rhode Island makes it a crime to use a computer to destroy evidence for the purpose of obstructing an official investigation.(73) Utah makes it an offense to fail to report a computer crime.(74)

III. PROPOSED LEGISLATION

{26}Some effort is being made to outlaw posting personal information about law enforcement officers on the Internet, as this Arizona bill illustrates: "It is unlawful for a person to knowingly make available on the World Wide Web the personal information of a peace officer if the dissemination of the personal information poses an imminent and serious threat to the peace officer's safety or the safety of the peace officer's immediate family and the threat is reasonably apparent to the person making the information available."(75) A California bill discusses the importance of preventing the disclosure of a peace officer's or appointed official's home address via the Internet.(76)

{27}An Ohio bill would make it a misdemeanor to let prisoners have access to the Internet unless they are participating in "an approved educational program with direct supervision that requires the use of the Internet for training or research" and the access is provided in accordance with rules to be established by the Department of Corrections.(77) And several states have introduced legislation that would criminalize "spamming," e.g., the sending of unsolicited email.(78) A New Jersey bill would increase the penalties for accessing and/or damaging a "home computer."(79) The legislative history of the provision explains that it is needed because the state's cybercrimes statutes currently do not provide sufficient protection for home computer owners who are victimized by hackers or crackers, since they tend to concentrate on intrusions and damage to commercial systems.(80)

IV. CONCLUSION

{28}A review of cybercrime legislation adopted by the various states of the United States of America is an instructive exercise, for several reasons. On the one hand, one would expect that, as one of the more technologically advanced countries in the world, the constituencies which comprise the United States of America would have adopted substantive cybercrime legislation that is at once comprehensive and uniform. Yet that is not the case: As the previous sections demonstrate, there is a great deal of variation-both in terms of coverage and in terms of approaches-in the cybercrime legislation adopted by the various states.

{29}This variation is no doubt the product of several factors. One factor is certainly the relative rapidity with which cybercrime has emerged as a distinctive problem; because cybercrime is such a new phenomenon, states, unsurprisingly, vary widely in the speed with which they have addressed the types of conduct which

can be defined as "cybercrime." Another factor is the ambiguity inherent in the whole concept of "cybercrime:" On the one hand, we are confronted with what seem to be entirely new kinds of criminal activity which requires the adoption of new substantive criminal legislation; on the other hand, one can argue that we are simply dealing with "old wine in new bottles," e.g., with the use of the Internet and computer technology to facilitate the commission of long-extant crimes such as fraud.(81) This ambiguity can, quite understandably, generate confusion and inaction among state legislators. And yet another factor is the complexity of the phenomena at issue; unlike much, if not most, of the criminal activity encountered in the "real world," the kinds of criminal activity that occur in cyberspace, in the "virtual world" can be quite complex and therefore can present significant challenges for legislators at both the state and federal level.

{30}However, while one can justify the gaps that currently exist in state cybercrime legislation, this is not a situation that should continue, especially not in a country that prides itself on its technological advancement and expertise. Gaps in the law-especially in the law applicable to cybercrimes-benefit those who engage in socially-unacceptable conduct to exploit innocent persons. While this is an unacceptable state of affairs in the real, physical world, the effects of this failure-to-legislate can be particularly egregious when one is dealing with the cyber-world, in which individuals can be victimized by strangers, by persons whom they have never met, as to whose existence and motives they may well be quite ignorant and therefore as to whom they have no reason to be on notice, to be on guard and to attempt to take protective measures. Indeed, one aspect of the cyber-world is the essential futility discrete individuals encounter when trying to protect themselves from the often-creative depredations of online offenders.

{31}Although the discrete states constituting the United States of America will necessarily encounter obstacles(82) in their attempts to protect their citizens from these depredations, the enactment of adequate substantive cybercrime legislation is a necessary first step in the process. It is also an important symbolic gesture for other nations of the world, many of which are quite lacking in substantive cybercrime legislation. If the entities that comprise the United States of America do not, for example, adopt legislation making it a criminal offense to disseminate a computer virus, how can they condemn other nations for their failure to do so?

{32}Ultimately, the adoption of substantive cybercrime legislation is a step taken toward recognizing that cybercrimes represent a new phenomenon in criminal activity: the globalization of criminal conduct.(83) And the globalization of criminal conduct is a phenomenon which all jurisdictions - national as well as sub-national - must combine to combat.

ENDNOTES

[*] Susan Brenner currently serves as Associate Dean & Professor of Law at the University of Dayton School of Law in Dayton, Ohio. She has studied the area of cybercrimes extensively and oversees a website that serves as a valuable resource to research in this area. Her webiste may be found at http://www.cybercrimes.net.

[1]. *See* U.S. CONST. art. I § 8 (listing the U.S. Congress' power to legislate in various areas); U.S. CONST. amend. X (stating "[T]he powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."). *See also* FINDLAW INTERNET LEGAL RESOURCES, U.S. CONSTITUTION: ARTICLE I; ARTICLE TEXT; ANNOTATIONS (last visited on Nov. 5, 2000) at http://caselaw.findlaw.com/data/Constitution/article01/; FINDLAW INTERNET LEGAL RESOURCES, U.S. CONSTITUTION TENTH AMENDMENT; AMENDMENT TEXT; ANNOTATIONS (last visited on Nov. 5, 2000) at

http://caselaw.findlaw.com/data/Constitution/amendment10/.

[2]. *See, e.g.*, Geraldine Szott Moohr, *The Federal Interest in Criminal Law*, 47 SYRACUSE L. REV. 1127, 1130 (1997) (noting that federal jurisdiction concerns the power of the national government to enact legislation, while deciding whether such legislation should be enacted if jurisdiction exists is a matter of policy). *See generally* NATIONAL GOVERNORS' ASSOCIATION, PRINCIPLES FOR STATE-FEDERAL RELATIONS, in POLICY POSITIONS (NATIONAL GOVERNORS' ASSOCIATION 1997), available at http://www.nga.org/Pubs/Policies/EC/prinpoli.asp (stating "Federal action should be limited to problems that are national in scope, where the national interest requires a universal or uniform solution, and should not merely address problems that are common to all states.").

[3]. *See, e.g.*, Andrew St. Laurent, *Reconstituting United States v. Lopez: Another Look at Federal Criminal Law*, 31 COLUM. J.L. & SOC. PROBS. 61, 65 (1997).

[4]. Cybercrimes can be prosecuted "under at least forty different federal [criminal] statutes." *See, e.g.*, 18 U.S.C. § 875(c) (1994); Michael Hatcher, et al., *Computer Crimes*, 36 AM. CRIM. L. REV. 397, 410 (1999).

[5]. 18 U.S.C. § 1030 (1994).

[6]. American Bar Association Task Force on the Federalization of Criminal Law, *Report: Report on the Federalization of Criminal Law*, 1998 A.B.A. SEC. CRIM. JUST. REP. 2, http://www.abanet.org/crimjust/fedreport.html.

[7]. The Model Penal Code is one of these model statutory collections. It was drafted by the American Law Institute and originally released in 1962. It was designed as a comprehensive substantive criminal code which states could employ as a model in revising and assembling their own criminal codes, and it was quite successful. According to some estimates, somewhere between thirty-four and thirty-six of the fifty states used the Model Penal Code as a guide in making revisions to their criminal codes. See Dannye Holley, The Influence Of The Model Penal Code's Culpability Provisions On State Legislatures: A Study Of Lost Opportunities, Including Abolishing The Mistake Of Fact Doctrine, 27 SW. U. L. REV. 229, 229 n.2 (1997).

[8]. *See, e.g., Uniform State Laws: A Discussion Focused On Revision Of The Uniform Commercial Code*, 22 OKLA. CITY U. L. REV. 257, 259 (Albert J. Rosenthal, Moderator 1997) (symposium discussion); Steven L. Schwarcz, *A Fundamental Inquiry Into The Statutory Rulemaking Process Of Private Legislatures*, 29 GA. L. REV. 909, 940 (1995).

[9]. CYBERCRIMES NET, MODEL STATE COMPUTER CRIMES CODE (1999) at http://www.cybercrimes.net. As noted above, the Model State Computer Crimes Code is an effort to draft a set of model cybercrime provisions which states can use in enacting their own cybercrime legislation. It contains model statutory provisions in each of the eight areas listed above, along with extensive commentary for each provision. The commentary explains the legislative drafting choices that underlie each provision, and cites authority—including statutes, case law and law review articles—documenting the reasons for those choices.

[10]. See, e.g., ALA. CODE § 13A-8-101 (1994); ALASKA STAT. § 11.46.985 (Michie 1998).

[11]. See, e.g., GA. CODE ANN. § 16-9-93 (1999 & Supp. 2000).

[12]. See, e.g., COL. REV. STAT. ANN. § 16-5-401(4.5)(b) (West 2000). Generally, these statutes tend to start the running of the applicable limitations period on the date when the commission of the cybercrime was discovered. But see VA. CODE ANN. § 18.2-152.9 (Michie 1996) (prosecution must be commenced before the earlier of five years after the commission of the last act in the course of conduct constituting the offense or one year after the commission of the offense and the perpetrator's identity are discovered by the state or by

the victim).

[13]. See, e.g., N.Y. PENAL LAW § 156.50 (McKinney 1998 & Supp. 2000); TEX. PENAL CODE ANN. § 33.03 (Vernon 1994 & Supp. 2000); W. VA. CODE ANN. § 61-3C-17 (Michie 2000). These provisions tend to make the defendant's reasonable belief that he/she had the right to access a system or access or manipulate data contained in a system a defense to charges such as unlawful intrusion or alteration of data.

[14]. *See, e.g.*, CAL. PENAL CODE § 777 (West 1999 & Supp. 2000).

[15]. *See, e.g.*, CONN. GEN. STAT. ANN. § 53a-261 (West 1994); N.H. Rev. STAT. ANN. § 649-B:6 (1996 & Supp. 2000); N. J. STAT. ANN. § 2C: 20-34 (West 1995); VA. CODE ANN. § 8.01-328.1(B) (Michie 1996).

[16]. *See, e.g.*, MICH. COMP. LAWS ANN. § 762.10b (West 1991 & Supp. 2000); N.Y. CRIM. PROC. LAW § 20.60 (McKinney 1984 & Supp. 2000); OKLA. STAT. tit. 21, § 1957 (1983 & Supp. 2000).

[17]. *See, e.g.*, ALA.CODE § 13A-6-110 (1994 & Supp 2000); MICH. COMP. LAWS ANN. § 750.145d (West 1991 & Supp. 2000).

[18].OHIO REV. CODE ANN. § 2901.11 (Anderson 1996 & Supp. 2000).

[19]. *See, e.g.*, DEL. CODE ANN. tit. 11, § 1112A (1995 & Supp. 1998).

[20]. *See* FLA. STAT. ch. 847.0135 (2000 & Supp. 2001); GA. CODE ANN. § 16-12-100.2 (1999 & Supp. 2000).

[21]. *See, e.g.*, 720 ILL. COMP. STAT. 5/16D4 (1993 & Supp. 2000); MINN. STAT. ANN. § 609.891 (West 1987 & Supp. 2000); NEB. REV. STAT. § 28-1343.01 (2000).

[22]. VA. CODE ANN. § 18.2-152.7 (Michie 1996 & Supp. 2000).

[23]. *See* ALA. CODE § 13A-11-8 (1994 & Supp 2000); ALASKA STAT. § 11.41.270 (Michie 1998); CAL. PENAL CODE § 646.9 (West 1999 & Supp. 2000); CONN. GEN. STAT. ANN. §§ 53a-182b, 183 (West 1994 & Supp 2000); LA. REV. STAT. ANN. § 14:40.2 (West 1997 & Supp. 2000); MASS. ANN. LAWS ch. 265 § 43 (Law. Co-op. 1992 & Supp. 2000); N.H. REV. STAT. ANN. § 644:4 (1996 & Supp. 2000); N.Y. PENAL LAW § 240.30 (McKinney 1998 & Supp. 2000); N.D. CENT. CODE § 12.1-17-07 (2000); OKLA. STAT. tit. 21, § 1173 (1983 & Supp. 2000); WASH. REV. CODE § 9A.46.110 (2000); WIS. STAT. ANN. § 947.0125 (1999); WYO. STAT. ANN. § 6-2-506 (2000). *See also* CAL. PENAL CODE § 422 (West 1999 & Supp. 2000) (offense to transmit "credible threat" even absent intent to carry out threat).

[24]. *See* ALA. CODE § 13A-11-8 (1994 & Supp 2000); ARIZ. REV. STAT. ANN. § 13-2921 (1989 & Supp. 2000); ARK. CODE ANN. § 5-41-108 (Michie 1997); DEL. CODE ANN. tit. 11, § 1311 (1995 & Supp. 1998); HAW. REV. STAT. § 711-1106 (1993 & Supp. 1999); LA. REV. STAT. ANN. § 14:40.2 (West 1997 & Supp. 2000); ME. REV. STAT. ANN. tit. 17-A, § 210-A (West 1983 & Supp. 2000); N.H. REV. STAT. ANN. § 644:4 (1996 & Supp. 2000); N.Y. PENAL LAW § 240.30 (McKinney 1998 & Supp. 2000); N.D. CENT. CODE § 12.1-17-07 (2000); WASH. REV. CODE § 9A.46.110 (2000); WIS. STAT. ANN. § 947.0125 (1999); WYO. STAT. ANN. § 6-2-506 (2000). *See also* MASS. ANN. LAWS ch. 265, § 43 (Law. Co-op. 1992 & Supp. 2000).

[25]. *See* CAL. PENAL CODE § 653m (West 1999 & Supp. 2000); KAN. STAT. ANN. § 21-4113 (1995 & Supp. 1999); MD. CODE ANN., CRIMES & PUNISHMENTS § 555A (1996); N.C. GEN. STAT. § 14-196 (1999 & Supp. 2000); N.D. CENT. CODE § 12.1-17-07 (2000).

[26]. People v. Munn, 688 N.Y.S.2d 384, 385-86 (N.Y. Crim. Ct. 1999).

[27]. *See, e.g.*, H.B. 345, 1999 Leg., 156th Sess. (N.H. 1999); A.B. 3506, 1998 Leg., 208th Sess. (N.J. 1998).

[28]. *See, e.g.*, ALA. CODE § 13A-6-110 (1994 & Supp 2000); CAL. PENAL CODE § 288.2 (West 1999); FLA. STAT. ch. 847.0135 (2000 & Supp. 2001); GA. CODE ANN. § 16-12-100.2 (1999 & Supp. 2000); 720 ILL. COMP. STAT. 5/11-6 (1993 & Supp. 2000); IND. CODE § 35-42-4-6 (1998); ME. REV. STAT. ANN. tit. 17-A, § 259 (West 1983 & Supp. 2000); MICH. COMP. LAWS ANN. § 750.145d (West 1991 & Supp. 2000); N.H. REV. STAT. ANN. § 649-B:4 (1996 & Supp. 2000); N.M. STAT. ANN. § 30-37-3.2 (Michie Supp. 2000); N.C. GEN. STAT. § 14-202.3 (1999); TENN. CODE. ANN. § 39-13-528 (1997 & Supp. 2000); VA. CODE ANN. § 18.2-374.3 (Michie 1996). *See also* DEL. CODE ANN. tit. 11, § 1112A (1995 & Supp. 1998).

[29]. *See, e.g.*, KAN. STAT. ANN. § 21-3510 (1995); MICH. COMP. LAWS ANN. § 750.145a (West 1991 & Supp. 2000).

[30]. *See, e.g.*, S.B. 1312, 1999 Leg., Reg. Sess. (Conn. 1999).

[31]. IND. CODE § 35-42-4-6 (1998).

[32]. *See, e.g.*, DEL. CODE ANN. tit. 11, § 1112A (1995 & Supp. 1998); FLA. STAT. ch. § 847.0135 (2000 & Supp. 2001); MD. CODE ANN., CRIMES & PUNISHMENTS § 419A (1996 & Supp. 2000); N.H. REV. STAT. ANN. § 649-B:3 (1996 & Supp. 2000); VA. CODE ANN. § 18.2-374.3 (Michie 1996).

[33]. *See, e.g.*, FLA. STAT. ch. § 847.0135 (2000 & Supp. 2001); GA. CODE ANN. § 16-12-100.2 (1999 & Supp. 2000); MD. CODE ANN., CRIMES & PUNISHMENTS § 419A (1996 & Supp. 2000); N.H. REV. STAT. ANN. § 649-B:3 (1996 & Supp. 2000); OKLA. STAT. tit. 21, § 1040.13a (1983 & Supp. 2000); VA. CODE ANN. § 18.2-374.3 (Michie 1996).

[34]. *See, e.g.*, CAL. PENAL CODE § 311.11 (West 1999); FLA. STAT. ch. § 847.0135 (2000 & Supp. 2001); GA. CODE ANN. § 16-12-100.2 (1999 & Supp. 2000); 720 ILL. COMP. STAT. 5/11-20.1 (1993 & Supp. 2000); IND. CODE § 35-42-4-4 (1998 & Supp. 2000); MD. CODE ANN., CRIMES & PUNISHMENTS § 419A (1996 & Supp. 2000); N.H. REV. STAT. ANN. § 649-B:3 (1996 & Supp. 2000); N.J. STAT. ANN. § 2C:24-4 (West 1995 & Supp. 2000); OKLA. STAT. tit. 21, § 1040.13a (1983 & Supp. 2000); 18 PA. CONS. STAT. ANN. § 6312 (West 1983 & Supp. 2000); TEX. PENAL CODE ANN. § 43.26 (Vernon 1994 & Supp. 2000); WYO. STAT. ANN. § 6-4-303. (2000).

[35]. *See, e.g.*, ALA. CODE § 13A-6-111 (1994 & Supp 2000); GA. CODE ANN. § 16-12-100.1 (1999 & Supp. 2000).

[36]. *See* 18 PA. CONS. STAT. ANN. § 6318 (West 1983 & Supp. 2000).

[37]. *See, e.g.*, IND. CODE ANN. § 35-43-2-3 (1998). *See also* ALA. CODE § 13A-8-102 (1994); ALASKA STAT. § 11.46.484 (Michie 1998); ARK. CODE ANN. § 5-41-104 (Michie 1997); CAL. PENAL CODE § 502 (West 1999 & Supp. 2000); COLO. REV. STAT. § 185.5102 (2000); CONN. GEN. STAT. ANN. § 53a-251 (West 1994 & Supp. 2000); DEL. CODE ANN. tit. 11, § 932 (1995 & Supp. 1998); FLA. STAT. ch. § 815.06 (2000); GA. CODE ANN. § 16-9-93 (1999 & Supp. 2000); IDAHO CODE § 18-2202 (Michie 1997); 720 ILL. COMP. STAT. 5/16D3, 5/15D7 (1993 & Supp. 2000); IOWA CODE § 716A.2 (1993); KAN. STAT. ANN. § 21-3755 (1995 & Supp. 1999); KY. REV. STAT. ANN. §§ 434.845, 434.850 (Michie 1999); ME. REV. STAT. tit. 17-A, § 432 (1983 & Supp. 2000); MD. CODE ANN., CRIMES & PUNISHMENTS § 146 (1996 & Supp. 2000); MASS. ANN. LAWS ch. 266, § 120F (Law. Co-op. 1992 & Supp. 2000); MICH. COMP. LAWS ANN. § 752.795 (1991 & Supp. 2000); MINN. STAT. ANN. § 609.891 (West 1987 & Supp. 2000); MO. ANN. STAT. § 569.099 (1999); MONT. CODE ANN. § 456311 (2000); NEB. REV. STAT. §§ 28-1343.01, -1347 (1995); NEV. REV. STAT. § 205.4765 (1997 & Supp. 1999); N.H. REV. STAT. ANN. § 638:17 (1996 & Supp. 2000); N.J. STAT. ANN. § 2C: 20-32 (West 1995); N.M. STAT. ANN. § 30-45-5 (Michie 1997 & Supp. 2000); N.Y. PENAL LAW §§

156.05, .06, .10 (McKinney 1998 & Supp. 2000); N.C. GEN. STAT. § 14-454 (1999 & Supp. 2000); OHIO REV. CODE ANN. § 2913.04 (Anderson 1996 & Supp. 2000); OKLA. STAT. tit. 21, § 1953 (1983 & Supp. 2000); OR. REV. STAT. § 164.377 (1993 & Supp. 1998); 18 PA. CONS. STAT. ANN. § 3933 (West 1983 & Supp. 2000); R.I. GEN. LAWS § 11-52-3 (1999 & Supp. 2000); TENN. CODE ANN. § 39-14-602 (1997); TEX. PENAL CODE ANN. § 33.02 (Vernon 1994 & Supp. 2000); UTAH CODE ANN. § 76-6-703 (1999); VT. STAT. ANN. tit. 13, § 4102 (1998 & Supp. 2000); WASH. REV. CODE § 9A.52.120 (2000); W. VA. CODE § 61-3C-5 (2000); WIS. STAT. § 943.70 (1996 & Supp. 2000); WYO. STAT. ANN. § 6-3-504 (Michie 1999). Hawaii lets the court dismiss a hacking charge if, "having regard to the nature of the conduct alleged and the nature of the attendant circumstances, it finds that the defendant's conduct did not actually cause harm or damage to any computer, computer system, computer network, or any of its data or software." HAW. REV. STAT. § 708-893 (1993).

[38]. *See, e.g.,* ARK. CODE ANN. § 5-41-104 (Michie 1997). *See also* ALA. CODE § 13A-8-102 (1994); ARIZ. REV. STAT. § 13-2316 (1989 & Supp. 2000); CAL. PENAL CODE § 502 (West 1999 & Supp. 2000); COL. REV. STAT. § 18-55-102 (West 2000); CONN. GEN. STAT. ANN. § 53a-251 (West 1994 & Supp. 2000); DEL. CODE ANN. tit. 11, §§ 934, 935 (1995 & Supp. 1998); FLA. STAT. ch. 815.05 (2000); GA. CODE ANN. § 16-9-93 (1999 & Supp. 2000); HAW. REV. STAT. § 708-892 (1993); IOWA CODE § 716A.3 (1993); IDAHO CODE § 18-2202 (Michie 1997); 720 ILL. COMP. STAT. 5/16D3, 5/16D4 (1993 & Supp. 2000); KAN. STAT. ANN. § 21-3755 (1995 & Supp. 1999); LA. REV. STAT. ANN. § 14:73.2 (West 1997); ME. REV. STAT. ANN. tit. 17-A, § 433 (West 1983 & Supp. 2000); MD. CODE ANN., CRIMES & PUNISHMENTS § 146 (1996 & Supp. 2000); MICH. COMP. LAWS ANN. §§ 752.795, .797 (West 1991 & Supp. 2000); MINN. STAT. ANN. § 609.891 (West 1987 & Supp. 2000); MISS. CODE ANN. § 97-45-9 (1999); NEB. REV. STAT. § 28-1343.01, -1345 (1995); NEV. REV. STAT. 205.4765 (1997 & Supp. 1999); N.H. REV. STAT. ANN. § 638:17 (1996 & Supp. 2000); N.J. STAT. ANN. § 2C:20-25 (West 1995); N.M. STAT. ANN. §§ 30-45-4, 5 (Michie 1997 & Supp. 2000); N.Y. PENAL LAW §§ 156.05, .20, .25, .26, .27 (McKinney 1998 & Supp. 2000); N.C. GEN. STAT. §§ 14-454, 455 (1999 & Supp. 2000); N.D. CENT. CODE § 12.1-06.1-08 (1997); OKLA. STAT. tit. 21, §§ 1953, 1958 (1983 & Supp. 2000); OR. REV. STAT. § 164.377 (1993 & Supp. 1998); 18 PA. CONS. STAT. ANN. § 3933 (West 1983 & Supp. 2000); R.I. GEN. LAWS § 11-52-3 (1999 & Supp. 2000); S.C. CODE ANN. § 16-16-20 (Law. Co-op. 1985 & Supp. 1999); TENN. CODE ANN. § 39-14-602 (1997); UTAH CODE ANN. § 76-6-703 (1999); VA. CODE ANN. § 18.2-152.4 (Michie 1996 & Supp. 2000); VT. STAT. ANN. tit. 13, § 4103 (1998 & Supp. 2000); WIS. STAT. § 943.70 (1996 & Supp. 2000); WYO. STAT. ANN. § 6-3-502 (Michie 1999).

[39]. *See, e.g.,* ALA. CODE § 13A-8-102 (1994); CONN. GEN. STAT. ANN. § 53a-251 (West 1994 & Supp. 2000); DEL. CODE ANN. tit. 11, § 935 (1995 & Supp. 1998); FLORIDA STAT. Ann. § 815.04 (West 2000); KY. REV. STAT. ANN. § 434.855 (Michie 1999); N.H. Rev. STAT. ANN. § 638:17 (1996 & Supp. 2000). *See also* N.Y. PENAL LAW § 156.35 (McKinney 1998 & Supp. 2000).

[40]. *See* N.Y. PENAL LAW § 156.10 (McKinney 1998 & Supp. 2000).

[41]. *See, e.g.,* CAL. PENAL CODE § 502 (West 1999 & Supp. 2000); 720 ILL. COMP. STAT. 5/16D3 (1993 & Supp. 2000); IOWA CODE ANN. § 716A.3 (1993); ME. REV. STAT. ANN. tit. 17-A, § 433 (West 1983 & Supp. 2000); MICH. COMP. LAWS ANN. § 752.795 (West 1991 & Supp. 2000); MINN. STAT. ANN. § 609.87 (West 1987); MISS. CODE ANN. § 97-45-9 (1999); NEB. REV. STAT. § 28.1344 (1995); NEV. REV. STAT. § 205.4765 (Michie 1999 Cum. Supp.); N.M. STAT. ANN. § 30-45-4 (Michie 1997 & Supp. 2000); N.C. GEN. STAT. § 14-454 (1999 & Supp. 2000); TENN. CODE ANN. § 39-14-602 (1997).

[42]. *See, e.g.,* S. 1077, 183d Leg. (Pa. 1999).

[43]. *See, e.g.,* ALASKA STAT. § 11.46.740 (Michie 1998); HAW. REV. STAT. § 708-891 (1993); N.M. STAT. ANN. § 30-45-4 (Michie 1997 & Supp. 2000).

[44]. *See, e.g.,* ALA. CODE § 13A-8-103 (1994); CONN. GEN. STAT. ANN. § 53a-251 (West 1994 & Supp. 2000); DEL. CODE ANN. tit. 11, § 936 (1995); FLA. STAT. ch. 815.05 (2000); IOWA CODE § 716A.3 (1993); LA. REV. STAT. ANN. § 14:73.3 (West 1997); MISS. CODE ANN. § 97-45-7 (1999 & Supp. 2000); MO. ANN. STAT. § 569.097 (West 1999); NEV. REV. STAT. 205.4765 (1997 & Supp. 1999); N.M. STAT. ANN. § 30-45-4 (Michie 1997 & Supp. 2000); S.C. CODE ANN. § 16-16-20 (Law. Co-op.1985 & Supp. 1999); W.VA. CODE § 61-3C-7 (2000); WIS. STAT. § 943.70 (1996 & Supp. 2000).

[45]. *See, e.g.,* CONN. GEN. STAT. ANN. § 53a-251 (West 1994 & Supp. 2000); DEL. CODE ANN. tit. 11, § 934 (1995); FLA. STAT. ch. 815.06 (2000); LA. REV. STAT. ANN. § 14:73.4 (West 1997); MISS. CODE ANN. § 97-45-5 (1999 & Supp. 2000); MO. ANN. STAT. § 569.099 (West 1999); NEV. REV. STAT. 205.477 (1997 & Supp. 1999); N.H. REV. STAT. ANN. § 638:17 (1996 & Supp. 2000); N.C. GEN. STAT. § 14-456 (1999 & Supp. 2000); OKLA. STAT. tit. 21, § 1953 (1983 & Supp. 2000); UTAH CODE ANN. § 76-6-703 (1999); W. VA. CODE § 61-3C-8 (2000); WYO. STAT. ANN. § 6-3-504 (1999).

[46]. *See, e.g.,* CONN. GEN. STAT. ANN. § 53a-251 (West 1994 & Supp. 2000); DEL. CODE ANN. tit. 11, § 936 (1995); IOWA CODE § 716A.3 (1993); LA. REV. STAT. ANN. § 14:73.3 (West 1997); MISS. CODE ANN. § 97-45-7 (1999 & Supp. 2000); N. H. REV. STAT. ANN. § 638:17 (1996 & Supp. 2000); N. J. STAT. ANN. § 2A:38A-3 (West 2000); W.VA. CODE § 61-3C-7 (2000).

[47]. *See* N. C. GEN. STAT. § 14-457 (1999 & Supp. 2000).

[48]. GA. CODE ANN. § 16-9-93 (1999 & Supp. 2000). *See also* ME. REV. STAT. ANN. tit. 17-A, § 432 (West 1983 & Supp. 2000) (criminalizing invasion of computer privacy); VA. CODE ANN. § 18.2-152.5 (Michie 1996); W. VA. CODE § 61-3C-12 (2000) (criminalizing invasion of privacy via computer).

[49]. KAN. STAT. ANN. § 21-3755 (1995 & Supp. 1999); MISS. CODE ANN. § 97-45-5 (1999 & Supp. 2000); MO. ANN. STAT. § 569.095 (West 1999); S.D. CODIFIED LAWS § 43-43B-1 (Michie 1997); W. VA. CODE § 61-3C-10 (2000).

[50]. *See, e.g.,* ARIZ. REV. STAT. § 13-2316 (1989 & Supp. 2000); ARK. CODE ANN. § 5-41-103 (Michie 1997); CAL. PENAL CODE § 502 (West 1999 & Supp. 2000); COL. REV. STAT. § 18-55-102 (2000); FLA. STAT. ch. 815.06 (2000); HAW. REV. STAT. § 708-891 (1993); IDAHO CODE § 18-2202 (Michie 1997); 720 ILL. COMP. STAT. 5/16D5 (1993 & Supp. 2000); KANSAS STAT. § 21-3755 (1995 & Supp. 1999); LA. REV. STAT. ANN. § 14:73.5 (West 1997); MICH. COMP. LAWS ANN. § 752.794 (West 1991 & Supp. 2000); MISS. CODE ANN. § 97-45-3 (1999 & Supp. 2000); MONTANA CODE § 45-6-311 (2000); NEV. REV. STAT. § 205.477 (1986 & Supp. 1999); N.J. STAT. ANN. § 2C: 20-25 (West 1995); N.M. STAT. ANN. § 30-45-3 (Michie 1997 & Supp. 2000); N.C. GEN. STAT. § 14-454 (1999 & Supp. 2000); N.D. CENTURY CODE § 12.1-06.1-08 (1997); OKLA. STAT. tit. 21, § 1953 (1983 & Supp. 2000); OR. REV. STAT. § 164.377 (1993 & Supp. 1998); R.I. GEN. LAWS § 11-52-7 (1999 & Supp. 2000); S.C. CODE ANN. § 16-16-20 (1976 & Supp. 1999); TENN. CODE ANN. § 39-14-602 (1997); UTAH CODE ANN. § 76-6-703 (1999); VT. STAT. ANN. tit. 13, § 4103 (1998 & Supp. 2000); VA. CODE ANN. §§ 18.2-152.3, .8 (Michie 1996); W. VA. CODE § 61-3C-4 (2000).

[51]. *See* COL. REV. STAT. § 185.5102 (West 2000).

[52]. *See, e.g.,* HAW. REV. STAT. § 708-891 (1993); N.M. STAT. ANN. § 30-45-3 (Michie 1997 & Supp. 2000).

[53]. *See, e.g.,* COL. REV. STAT. § 185.5102 (West 2000); GEORGIA CODE § 16993 (1999 & Supp. 2000); IDAHO CODE § 18-2202 (Michie 1997); IOWA CODE § 716A.9 (1993); MINN. STAT. ANN. § 609.89 (West 1987 & Supp. 2000); N.J. STAT. ANN. § 2C: 20-25 (West 1995); R.I. GEN. LAWS § 11-52-4 (1999 & Supp. 2000); VT. STAT. ANN. tit. 13, § 4105 (1998 & Supp. 2000).

[54]. *See, e.g.*, COL. REV. STAT. § 18-4-412 (West 2000); IOWA CODE § 716A.9 (1993); MINN. STAT. ANN. § 609.89 (West 1987 & Supp. 2000); N.J. STAT. ANN. § 2C:20-25 (West 1995); R.I. GENERAL LAWS § 11-52-4 (2000).

[55]. *See, e.g.*, MINN. STAT. ANN. § 609.89 (West 1987 & Supp. 2000); N.J. STAT. § 2C: 20-25 & 2C: 20-33 (1995); R.I. GENERAL LAWS § 11-52-4 (2000).

[56]. *See, e.g.*, N.J. STAT. § 2C: 20-25 (1995); R.I. GENERAL LAWS § 11-52-4 (2000).

[57]. *See, e.g.*, CONN. GEN. STAT. ANN. § 53a-251 (West 1994 & Supp. 2000); DEL. CODE ANN. tit. 11, § 933 (1995); IOWA CODE § 716A.9 (1993); MASS. ANN. LAWS ch. 266, § 33A (Law. Co-op. 1992 & Supp. 2000); N.H. REV. STAT. ANN. § 638:17 (1996 & Supp. 2000); VA. CODE ANN. § 18.2-152.6 (Michie 1996).

[58]. *See, e.g.*, ALA. CODE § 13A-8-102 (1994); COL. REV. STAT. § 185.5102 (West 2000); CONN. GEN. STAT. ANN. § 53a-251 (West 1994 & Supp. 2000); GEORGIA CODE § 16993 (1999 & Supp. 2000); HAW. REV. STAT. § 708-891 (1993); IDAHO CODE § 18-2202 (Michie 1997); IOWA CODE § 716A.9 (1993); KANSAS STAT. § 21-3755 (1995 & Supp. 1999); KY. REV. STAT. ANN. § 434.845 (Michie 1999); LA. REV. STAT. ANN. § 14:73.2 (West 1997); MICH. COMP. LAWS ANN. § 752.796 (West 1991 & Supp. 2000); MINN. STAT. ANN. § 609.89 (West 1987 & Supp. 2000); MISS. CODE ANN. § 97-45-9 (1999); MO. ANN. STAT. § 569.097 (West 1999); MONTANA CODE ANN. § 45-6-311 (2000); NEB. REV. STAT. § 28-1344 (1995); N.H. REV. STAT. § 638:17 (1996); N.J. STAT. ANN. §§ 2C:20-25, -33 (West 1995); N.M. STAT. §§ 30-45-3 (1997 & 2000); OR. REV. STAT. § 164.377 (1993 & Supp. 1998); S.C. CODE ANN. § 16-16-20 (Law. Co-op. 1985 & Supp. 1999); UTAH CODE ANN. § 76-6-703 (1999); VA. CODE ANN. § 18.2-152.3 (Michie 1996); W. VA. CODE § 61-3C-4 (2000).

[59]. *See, e.g.*, W. VA. CODE § 61-3C-6 (2000).

[60]. *See, e.g.*, ARK. CODE ANN. § 5-37-227 (Michie 1997); GA. CODE ANN. § 16-9-121 (1999 & Supp. 2000); KAN. STAT. ANN. § 21-4108 (1995); MD. CODE ANN., CRIMES & PUNISHMENTS § 231 (1996 & Supp. 2000); MASS. ANN. LAWS ch. 266, § 33E (Law. Co-op. 1992 & Supp. 2000); OKLA. STAT. tit. 21, § 1533.1 (1983 & Supp. 2000); WASH. REV. CODE § 9.35.020 (2000).

[61]. *See, e.g.*, GA. CODE ANN. § 16-9-121 (1999 & Supp. 2000). *See also* NEV. REV. STAT. 205.481 (1997 & Supp. 1999); VA. CODE ANN. § 18.2-152.14 (Michie 1996); W. VA. CODE § 61-3C-15 (2000).

[62]. N.J. STAT. ANN. § 2C: 21-1 (West 1995).

[63]. *See* LA. REV. STAT. ANN. § 14:90.3 (West 1997).

[64]. *See id.*

[65]. *See, e.g.*, H.R. B. 2907, 91st Gen. Assem., Reg. Sess. (Ill. 1999) (criminalizing wire transfers of money if the money is to be used as part of an Internet-based gambling transaction); H.R. B. 1484, 111th Gen. Assem., Reg. Sess. (Ind. 1999) (would make Internet gambling a misdemeanor).

[66]. *See* 235 ILL. COMP. STAT. 5/6-29.1 (1993 & Supp. 2000).

[67]. *See, e.g.*, H. B. 293, 140th Gen. Assem., Reg. Sess. (Del. 1999); H. B. 6346, 1999-2000 Leg. Sess. (R.I. 1999).

[68]. *See, e.g.*,S. B. 5951, 222nd Leg. Sess. (N.Y. 1999).

[69]. 720 ILL. COMP. STAT. 5/16D4 (1993 & Supp. 2000).

[70]. *See* W. VA. CODE § 61-3C-14 (2000); NEV. REV. STAT. 205.4765 (1997 & Supp. 1999).

[71]. NEB. REV. STAT. § 28-1346 (1995); W. VA. CODE § 61-3C-11 (2000).

[72]. *See* W. VA. CODE § 61-3C-4 (2000).

[73]. *See* R.I. GEN. LAWS § 11-52-8 (1999 & Supp. 2000).

[74]. *See* UTAH CODE ANN. § 76-6-705 (1999).

[75]. *See, e.g.*, S. B. 1279, 1999 Leg., 44th Sess. (Ariz. 1999). *See also* MODEL STATE COMPUTER CRIMES CODE § 8.06.01 (1999), *at* http://www.cybercrimes.net.

[76]. *See* A. B. 151 Gen. Assem., 1999-2000 Reg. Sess. (Calif. 1999).

[77]. *See* S. B. 12, 123rd Gen. Assem., Reg. Sess. (Ohio 1999).

[78]. *See, e.g.*, H. B. 6443, Gen. Assem, 1999 Reg. Sess. (Conn. 1999); H. B. 242, 140th Gen. Assem., Reg. Sess. (Del. 1999); H. B. 1287, Gen. Assem., 1999 Reg. Sess. (N.C. 1999).

[79]. *See* A. B. 3258, 208th Leg., Reg. Sess. (N.J. 1998).

[80]. *See id.*

[81]. *See, e.g.*, Susan W. Brenner, *Can There Be Truly Virtual Crimes?*, http://www.cybercrimes.net/Virtual/Brenner.html.

[82]. *See, e.g.*, Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465 (1997), at http://jolt.law.harvard.edu/low/articles/10hjolt465.html.

[83]. The author has, for example, received e-mails from individuals located within the United States and in other countries which complain about having been victimized by cybercriminals who engaged in similar conduct. In some instances, the author was able to refer the author of the e-mail to United States of America laws which outlawed the conduct at issue; in other instances, she was not able to refer the author of the e-mail to such law, either because it was lacking in a constituent state of the United States of America or because it was lacking in another country. Regardless of where the victim is located, this is a tragic state of affairs.

Related Browsing

1. http://www.techtv.com/cybercrime.TechTV, CyberCrime. This is a website targeted to the general population that discusses cybercrime current events and legal inquiries concerning the Internet. The information is fairly general and wide ranging.

2. http://www.usdoj.gov/criminal/cybercrime/index.html The United States Department of Justice. This is a resource page with links to cases, laws, policy, and documents pertaining to cybercrime. It includes information about computer crime, intellectual property crime, and cybercrime with direction as to how to

report cybercrime.

3. http://www.cybercrimes.net/Seminar/Public/Discussions/discussion4.html. Susan Brenner's website. This is a discussion moderated and lead by Brenner discussing whether cybercrimes should be dealt with at the state or federal level. It includes her original question and responses by students to the issue.

4. http://www.cybercrimes.net/99MSCCC/. Susan Brenner's website. This is a brief discussion by Brenner about why states have different kinds of cybercrime laws.

5. http://cve.mitre.org/. Common Vulnerabilities and Sharing: The Key to Information sharing. A list of standardized names for vulnerabilities and other information security exposures. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.

6. http://www.cyberangels.org/. CyberAngels.org. Internet safety volunteer organization fights cybercrime and empowers users through safety education.

7. http://cyber.findlaw.com/. Find Law. Cyber Space Law Center. Resources for legal issues concerning cyberspace.

8. http://www.iipa.co.uk/. Internet Investigation & Protection Authority. Home of the recently established UK Internet Authority. Information on laws governing Internet content, and how to report illegal sites. The IIPA is not a government agency.

9. http://www.gseis.ucla.edu/iclp/97cases.html. Top Cyberspace Law Cases of 1997. Twelve cases are examined by Prof. Jerry Kang at the Cyberspace Law & Policy Institute.

10. http://www.web-police.org/. Web Police. Offers law enforcement and crime prevention services specifically for the Internet and cybercrimes with online form to report crimes.

11. http://www.identitytheft.org/. Identity Theft. Advice, articles and products for victims of online fraud.

12. http://www.jimcarroll.com/articles/70.htm. Personal Privacy Online by Jim Carroll. A look at all the Web services that solicit personal information without explaining how they intend to use it.
