Volume 91 | Issue 2 Article 13

January 1989

Computer Crime in West Virginia: A Statutory Proposal

Jeffry A. Pritt
West Virginia University College of Law

COMPUTER CRIME IN WEST VIRGINIA: A STATUTORY PROPOSAL

I. INTRODUCTION 569
II. COMPUTER CRIME 570
III. THE NEED FOR A STATUTE 573
IV. THE PROPOSED WEST VIRGINIA COMPUTER CRIMES ACT 576
V. PROPOSED SECTIONS AND COMMENTS 577
A. *Title, Purpose, and Definitions* 577
B. *Computer Fraud, Computer Trespass, and Offense Against Intellectual Property* 580
C. *Penalties, Presumptions, and Venue* 584
D. *Civil Actions* 588
E. *Severability and Assistance of Attorney General.* 589
VI. CONCLUSION 589
APPENDIX 591

I. INTRODUCTION

It is all too apparent to even the casual observer in this modern day and age that the computer plays an integral part in the life of every individual. From the withdrawal of money at an automated teller machine to the scanning devices that check prices on foodstuffs at the local supermarket, computers and their related systems touch our lives every day.[1] And as if all the involuntary contact we have with computers day in and day out is not enough, it is now quite common to find a personal computer in a large proportion of the homes in this country. Sales of such personal computers were expected to exceed 16 million units in 1988.[2] And by the year 2000, some twenty percent of the American population may "telecommute" by working "from the comfort of their homes via their com-

1. *See generally* Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMPUTER L.J. 353 (1980).

2. A. BEQUAI, TECHNOCRIMES 4 (1987).

puters."[3] Even now, many personal computer users frequently communicate with each other by computer over the telephone.[4] And for a more diversified exchange of ideas with a number of different people at the same time, one can dial up an electronic "bulletin board,"[5] some 1,000 to 5,000 of which are ready to be accessed at almost any time.[6]

We are living in an age where the free exchange of information and ideas has reached a point unparalleled in human history. Modern man is becoming increasingly reliant on the computer to handle an ever-widening array of tasks in a much faster and precision-like manner than was ever before possible. Even West Virginia, a rural state historically dependent upon only a few major industries, is feeling the changes inherent in the growth and momentum of this high-tech revolution. However, the overwhelming benefits of the computer age have been accompanied by significant and alarming developments on the darker side of this revolution.[7]

II. Computer Crime

What is computer crime? Unfortunately, no two definitions are quite the same. However, at least a couple of very general observations are not in contention. In the broadest sense, it is white-collar crime[8] and encompasses any crime committed with the aid of

---

3. *Id.*

4. Any computer user who has a modem, a device which converts information into electrical pulses for transmission, can communicate with any other computer similarly equipped by using regular telephone transmission lines.

5. Electronic bulletin boards are a modern version of the old community bulletin board. Operated by a very dedicated computer buff who has the necessary leisure time to devote to such a time-consuming activity, they require specialized computer programming which allows many different users to access the system and leave or exchange various types of information depending upon a board's particular orientation. Some of these boards can be freely accessed by anyone, but the majority do require some type of access code to gain entry past their initial welcoming stage. *See generally* Soma, Smith, & Sprague, *Legal Analysis of Electronic Bulletin Board Activities*, 7 W. New Eng. L. Rev. 571 (1985); Comment, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 Fed. Comm. L.J. 217 (1987).

6. Allen, *Bulletin Boards of the 21st Century are Coming of Age*, Smithsonian, Sept. 1988, at 83, 86-88.

7. A. Bequai, *supra* note 2, at x.

8. For a "broad outline" of the typical computer criminal who is young, intelligent, and skilled in computer use, see Sokolik, *supra* note 1, at 365-366; Volgyes, *The Investigation, Prosecution, and Prevention of Computer Crime: A State- of-the-Art Review*, 2 Computer L.J. 385, 387 (1980); S. Wolk & W. Luddy, Jr., Legal Aspects of Computer Use 121-22 (1986).

a computer.[9] It can also be said that just as our use of computers has continued to grow in recent times, so too has the number and variety of computer crimes. Such crimes can range from the astonishingly sophisticated, such as Japan's Hitachi combining with the National Semiconductor Corporation to steal high-tech information from IBM which was valued between $750 million and $2.5 billion,[10] to the surprisingly simple, such as the housewife who watched the television program *60 Minutes*, and in the process learned "how easy it was to steal by computer . . . taking People's Security Bank for more than $36,000."[11]

Computer crime can be divided into three main categories: sabotage, in which the computer or its system is attacked by either physical means or programming methods such as a "virus;"[12] theft of computer services, in which the main goal is to use the services of a computer or its system without paying; and property crimes, which involve the theft of property (including such intangible items as data stored in a computer's memory).[13]

Why is such crime on the increase? Several factors are responsible. Some experts maintain that the technical knowledge necessary to carry out some computer-related crime is not that complex.[14] They conclude that computer crime is within the grasp of almost anyone who has access to a keyboard.[15] There is also the fear that too little

---

9. M. ROSTOKER & R. RINES, COMPUTER JURISPRUDENCE 332 (1986); A. BEQUAI, *supra* note 2, at 47.

10. A. BEQUAI, *supra* note 2, at 50.

11. *Id.* at 49.

12. A "virus" is an especially destructive form of computer program that can disrupt the operation and destroy much of the memory of a computer system. Such programs are a severe threat because they can be designed to spring into destructive action at any point in the future, while presently being transferred from, and thus "infecting", one computer system after another in an undetected, dormant form. Since the actual construction of these "viruses" can vary greatly, there is no certain way at present to protect a particular computer system other than completely cutting it off from all outside information sources or disks. *See generally* Elmer-DeWitt, *Invasion of the Data Snatchers!*, TIME, Sept. 26, 1988, at 62.

13. S. WOLK & W. LUDDY, JR., *supra* note 8, at 117. *See generally* Reimer, *Judicial and Legislative Responses to Computer Crimes*, 53 INS. COUNS. J. 406, 407-09 (1986). *See also* Volgyes, *supra* note 8, at 388-389 (for some varying definitions of the types of computer crime).

14. A. BEQUAI, *supra* note 2, at 49-50.

15. In fact, one early report found that most computer criminals had a limited technical knowledge of computers. Volgyes, *supra* note 8, at 393.

attention has been paid to the security aspect of computer systems in both the public and private sectors.[16] Simply put, the money and effort devoted to training and employing security personnel has lagged as technological knowledge has rapidly advanced in the last several years.[17]

Then there is the problem of detection. Unfortunately, most computer crime is discovered only by accident.[18] Once a computer criminal has bypassed the security barriers of a system, there is little chance that he will ever be caught. In fact, it has been estimated that for every computer crime detected, one hundred incidents are never discovered.[19]

Compounding the detection problem is the belief that a high percentage of discovered computer crime is never reported to authorities.[20] It could be highly embarrassing, not to mention unprofitable, for any business enterprise to admit a breach of computer security.[21] The repercussions of such an admission could be particularly devastating to those firms involved in matters that require a high degree of security. For this reason, many believe that a significant amount of computer crime is simply brushed under the rug, rendering unreliable any estimate as to the true extent of the problem.

Despite uncertainty regarding its full extent, it generally can be agreed that computer crime is expensive. Some estimates place the average loss per occurrence at $400,000,[22] and figures as to the annual cost of such crime range between $100 million and $5 billion.[23] Accepting even the lowest of these figures, it is obvious that computer crime is a major problem in this country.

---

16. Sokolik, *supra* note 1, at 368.

17. Note, *Computer Crime*, 22 AM. CRIM. L. REV. 494, 500 (1984).

18. M. ROSTOKER & R. RINES, *supra* note 6, at 354; Note, *Addressing Computer Crime in Massachusetts: The Problems with Comprehensive New Criminal Statutes—The Advantages to a Multifaceted Approach*, 21 NEW ENG. L. REV. 759, 764 (1987); Sokolik, *supra* note 1, at 359; A. BEQUAI, *supra* note 2, at 56.

19. Reimer, *supra* note 13, at 406.

20. Note, *supra* note 18, at 764; Note, *supra* note 17, at 500; Sokolik, *supra* note 1, at 359.

21. A. BEQUAI, *supra* note 2, at 113.

22. *Id.* at 119.

23. *Id.* at 50-52; Reimer, *supra* note 13, at 406; Volgyes, *supra* note 8, at 386-87.

III. The Need For A Statute

In response to the increasing concern over the escalating cost of computer crime, most states have proceeded with some sort of legislative response.[24] A few states have attempted to alleviate this threat by altering their respective statutory definitions of property to include such intangible items as information stored inside a computer.[25] Thus, prosecution for some types of computer crime can be attempted in such states under conventional criminal statutes.[26] Other states, beginning in 1978 when Florida passed the first computer crimes act,[27] have specifically addressed the somewhat complicated issues of such crime.[28] Only two states, including West Virginia, have failed to confront this problem. The other forty-eight have adopted some type of legislation that addresses the issue of computer crime in one of the two ways previously mentioned.[29]

---

24. On the federal level, Congress enacted the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, 18 U.S.C. 1030 (Supp. IV 1986). However, this statute is very limited in scope and only protects United States government computers and information. *See* Tompkins, Jr. & Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem*, 6 COMPUTER L.J. 459 (1986); M. ROSTOKER & R. RINES, *supra* note 9, at 347. Therefore, there currently is no comprehensive computer crime bill on the national level and consequently, regulation in this area is the responsibility of the various states.

25. Note, *supra* note 18, at 767.

26. However, as per the overall theme of this note, this is not the best approach to the problem since existing law, when used for the prosecution of a computer crime, will still be inadequate to address some of the particular forms of this type of crime such as the copying of data or programs.

27. FLA. STAT. ANN. §§ 815.02 to .07 (West Supp. 1988).

28. *See generally* Note, *supra* note 18 (for criticism of these various acts).

29. ALA. CODE §§ 13A-8-100 to -103 (Supp. 1987); ALASKA STAT. §§ 11.46.200(a)(3), .740, .985, .990(1), (3)-(7) (Supp. 1986); ARIZ. REV. STAT. ANN. §§ 13-2301(E), 13-2316 (1978); ARK. STAT. ANN. §§ 5-41-101 to -107 (Supp. 1987); CAL. PENAL CODE 502 (Deering Supp. 1988); COLO. REV. STAT. §§ 18-5.5-101 to -102 (1986); CONN. GEN. STAT. ANN. §§ 53a-250 to -261 (West 1985); DEL. CODE ANN. tit. 11, §§ 931-939 (1987); FLA. STAT. ANN. §§ 815.01 to .07 (West Supp. 1988); GA. CODE ANN. §§ 16-9-90 to -95 (1984); HAW. REV. STAT. §§ 708-890 to -896 (1985); IDAHO CODE §§ 18-2201 to -2202 (1987); ILL. ANN. STAT. ch. 38, para. 16D-1 to -7 (Smith-Hurd Supp. 1988); IND. CODE ANN. §§ 35-43-1-4 to -2-3 (Burns Supp. 1988); IOWA CODE ANN. §§ 716A.1 to .16 (West Supp. 1988); KAN. STAT. ANN. § 21-3755 (Supp. 1987); KY. REV. STAT. ANN. §§ 434.840 to .860 (Michie/Bobbs-Merrill 1985); LA. REV. STAT. ANN. §§ 73.1to .5 (West 1986); MD. ANN. CODE art. 27, § 146 (1987); MASS. GEN. LAWS ANN. ch. 266, § 30 (West 1987); ME. REV. STAT. ANN. tit. 17-A, § 357 (1983); MICH. STAT. ANN. §§ 28.529(1) to (7) (Callaghan 1981); MINN. STAT. ANN. §§ 609.87 to .89 (West 1987); MISS. CODE ANN. §§ 97-45-1 to -13 (Supp. 1987); MO. ANN. STAT. §§ 569.093 to .099 (Vernon Supp. 1988); MONT. CODE ANN. §§ 45-2-101(54)(k), -101(69)(a)(iii), & 45-6-310 to -311 (1987); NEB. REV. STAT. §§ 28-1343 to -1348 (1985); NEV. REV. STAT. §§ 205.473 to .477 (1987); N.H. REV. STAT. ANN. §§ 638:16 to :19 (1986); N.J. STAT. ANN. §§ 2A:38A-1 to -6 (West 1987); N.M. STAT. ANN. §§ 30-16A-1 to -4 (1988); N.Y. PENAL LAW §§ 156.00 to .50 (McKinney Supp. 1988); N.C. GEN. STAT. §§ 14-

Current West Virginia law would be inadequate to effectively prosecute many forms of computer crime,[30] perhaps the most important reason that other states have passed such laws. While it is clear that crimes consisting of the actual theft or physical destruction of a computer would be sufficiently covered by existing laws,[31] questions arise in the instance of unauthorized copying of data or computer programs in which no one is deprived of possession, and yet obviously a theft of a different sort has occurred.[32] A properly written computer crime statute need not preclude the applicability of existing law,[33] yet it could define the illegality of conduct peculiar to the abuse of computers, such as the copying of data or the accessing and use of a computer system without authorization.

Also, a statute directly addressing computer crime could result in greater deterrence, certainly important when considering any form of white-collar crime. Conceding the great chance of success for the typical white-collar worker committing this kind of crime,[34] such acts

---

453 to -457 (1986); N.D. CENT. CODE §§ 12.1-06 to .1-08 (Supp. 1987); OHIO REV. CODE ANN. §§ 2901.01(J), 2913.01(L) (Page Supp. 1987); OKLA. STAT. ANN. tit. 21, §§ 1951-1955 (West Supp. 1988); OR. REV. STAT. § 164.377 (1987); 18 PA. CONS. STAT. ANN. § 3933 (Purdon Supp. 1988); R.I. GEN. LAWS §§ 11-52-1 to -5 (Supp. 1987); S.C. CODE ANN. §§ 16-16-10 to -40 (Law. Co-op. 1985); S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to -8 (Supp. 1988); TENN. CODE ANN. §§ 39-3-1401 to -1406 (Supp. 1987); TEX. PENAL CODE ANN. §§ 33.01 to .05 (Vernon Supp. 1988); UTAH CODE ANN. §§ 76-6-701 to -705 (Supp. 1987); VA. CODE ANN. §§ 18.2-152.1 to -152.14 (1988); WASH. REV. CODE ANN. §§ 9A.48.100, .52.110 to .130, .56.010 (1988); WIS. STAT. ANN. § 943.70 (West Supp. 1987); WYO. STAT. §§ 6-3-501 to -505 (1988).

30. For example, a larceny prosecution in West Virginia under W.VA. CODE § 61-3-13 (1984), requires that the property of another be taken and carried away with the intent to deprive the owner of possession. *See* State v. Houdyshell, 329 S.E.2d 53, 55 (W. Va. 1985). When information is copied from a computer, nothing is actually taken and the owner is almost never deprived of possession. Thus prosecution for such a theft under existing West Virginia law would be extremely difficult. Further, the definition of "personal property" in W. VA. CODE § 2-2-10 (1981), which includes "goods, chattels, real and personal, money, credits, investments and the evidences thereof" is not conclusive as to whether intangibles, such as data stored inside a computer, is encompassed within the term.

31. Obviously, when a computer or any other related tangible item is physically harmed, any existing law pertaining to the destruction of property will apply depending upon the particular facts of the situation.

32. *See generally* Reimer, *supra* note 13, at 411-18 (for a discussion of some of the more often mentioned computer crime cases prosecuted under conventional criminal codes).

33. There are bound to be instances in which existing statutes will be more appropriate for prosecution in a particular case than a specific computer crime statute. *See* M. ROSTOKER & R. RINES, *supra* note 9, at 345; Ingraham, *On Charging Computer Crime*, 2 COMPUTER L.J. 429, 438 (1980).

34. *See* Becker, *The Trial of a Computer Crime*, 2 COMPUTER L.J. 441, 455 (1980) (noting that historically, even when a computer criminal is prosecuted and convicted, the sentence is usually light).

would probably be curbed if they were clearly delineated as punishable offenses. Many computer criminals may not view their acts as wrong where the only harm inflicted is to impersonal corporations. However, the threat of prosecution might compel consideration of the serious nature of this type of activity.

Enhancement of prosecution is the single most important factor supporting computer crime legislation.[35] Prior to enactment of the various state laws, it was thought that prosecutors sometimes turned down cases of this nature due to difficulties inherent in prosecuting them under conventional law.[36] There is no doubt that an effectively worded statute would ease this burden. However, a prime criticism of computer crime statutes is that, though they have been touted as making conviction easier, prosecutors have rarely utilized them after adoption. For example, Texas recently prosecuted its first case under a computer crime statute which had been on its books for three years.[37] The small number of prosecutions may simply reflect the detection and reporting problems previously discussed, although at least one computer crime act contained a statutory flaw.[38]

Though some commentators have argued that computer crime statutes are overbroad and ill-defined,[39] the sheer magnitude of the problem mandates a legislative response. Although comprehensive computer crime statutes have yet to stand the test of time and certainly contain flaws which will be revealed as their use increases, the basic fact remains that under existing West Virginia law, prosecution would be difficult. Therefore, the most sensible approach is to enact a West Virginia Computer Crimes Act specifically ad-

35. Sokolik, *supra* note 1, at 374-75.

36. *See* Reimer, *supra* note 13, at 409 (noting that under many potentially applicable sections of existing state criminal codes such as "arson, conversion, criminal mischief, burglary, larceny, theft of trade secrets, embezzlement, receipt of stolen property, theft of services or labor under false pretenses, forgery, interference with use of property, and conspiracy," prosecutors had trouble prosecuting persons for computer crime). *See also* A. BEQUAI, *supra* note 2, at 116; Sokolik, *supra* note 1, at 375-78; BloomBecker, *Computer Crime Update: The View As We Exit 1984*, 7 W. NEW ENG. L. REV. 627, 645 (1985) (noting the small number of computer crime cases actually tried).

37. Wall St. Journal, Sept. 21, 1988, at A13, col. 3; Elmer-DeWitt, *supra* note 12, at 63.

38. A rather critical error was found in the Utah Computer Crime Act that might have inhibited prosecutions. *See* Note, *Utah Legislative Survey*, 1980 UTAH L. REV. 155, 177-181 (1980).

39. Note, *supra* note 18, at 759, 767-68; S. MANDELL, COMPUTERS, DATA PROCESSING, AND THE LAW 166 (1986).

West Virginia Law Review, Vol. 91, Iss. 2 [1989], Art. 13

dressing the problem in an effective manner. This note will consider the form of such an act and offer a brief analysis of its various sections.

IV. The Proposed West Virginia Computer Crimes Act

While in many areas of the law there are statutes which are basically similar in form from one state to another as well as model or uniform codes in some fields, states have enacted a variety of provisions in response to computer crime. While there is no model computer crime statute,[40] there are some similarities found among the various states' computer crime acts.

Therefore, in formulating a proposed computer crime act for West Virginia, the statutory law in other states pertaining to this type of crime was reviewed and evaluated. The result is a synthesis of the best existing law in the field for adoption in West Virginia. The proposed act for West Virginia is not unique; yet as a compilation of various provisions, it is somewhat different. This approach provides distinct advantages.

Despite the absence of a model code in this area of the law, some parts of the various computer crime acts exhibit considerable uniformity.[41] By using these portions in West Virginia's act, uniformity would be maintained, and sections of code not common to a large number of the states, when adopted for use in West Virginia, would at least be shared with one other jurisdiction. Therefore, there is an increased possibility that a particular section of the West Virginia act will have been construed previously, although by a court in another jurisdiction. West Virginia courts could find this beneficial when they finally do face the complex and highly technical aspects of computer crime.

The question of construction is also important when considering the low number of prosecutions under this type of legislation and

40. Note, *supra* note 18, at 767.

41. This is due in part to the use of some portions of the Federal Computer Systems Protection Act of 1979 as a partial model code. The Act, S.240, was introduced by Sen. Ribicoff on Jan. 25, 1979, although it did not pass Congress. S.240, 96thCong., 1st Sess., 125 Cong. Rec. S711 (daily ed., Jan. 25, 1979).

the consequent lack of case law.[42] By using some of the better portions of other state statutes, there is greater chance that other jurisdictions will make some analysis to which the West Virginia courts can refer if necessary.

Finally, if there is an error of any type in the proposed statute, since it is adopted completely from the existing law of other states, there is a greater chance that such a mistake will be found in another jurisdiction, and West Virginia will have an opportunity to correct the flaw. Of course, with the current trend of technological acceleration, there is a good possibility that an act of this type will need some adjustment within the not too distant future despite any current flexibility and application.

V. Proposed Sections and Comments

A. Title, Purpose, and Definitions

§ 61-3C-1. Title.
This article shall be known by the short title of "The West Virginia Computer Crimes Act."

§ 61-3C-2. Legislative purpose.
It is found and determined that computer-related crime poses a major problem for business and government; that losses for each incident of computer-related crime are potentially astronomical; that the opportunities for computer-related crime in business and government through the introduction of fraudulent records into a computer system, the unauthorized use of computers, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great; that computer-related crime has a direct effect on state commerce; and that, while various forms of computer crime might possibly be the subject of criminal charges based on other provisions of the law, it is appropriate and desirable that a statute be enacted which deals directly with computer crime.

Comment: The first section set out above, § 61-3C-1, is simply the short title of the act. The second part, the legislative purpose, presents a succinct summary of the reasons for enacting this article.[43] Since the West Virginia Computer Crimes Act would be a proscrip-

42. Reimer, *supra* note 13, at 407.

43. This type of stated legislative purpose is present in several state codes in this basic form. *See, e.g.*, Ark. Stat. Ann. § 5-41-101 (Supp. 1987).

tion against a certain kind of criminal behavior, it obviously belongs in chapter 61 of the West Virginia Code [hereinafter W. Va. Code] which encompasses "Crimes and their Punishment." As for a particular placement within chapter 61, computer crime is most closely related to article 3 of chapter 61, "Crimes against property." Articles 3A and 3B, proscribing shoplifting and trespassing, respectively, follow article 3. Therefore, this article, dealing with computer crime, most logically should be added to the Code as article 3C of chapter 61.

§ 61-3C-3. Definitions.

The following words when used in this article have the meaning hereinafter ascribed to them, unless the context clearly indicates a different meaning:

(a) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise make use of any resources of, a computer, computer system, or computer network;

(b) "Authorization" means the express consent of a person, which may include an employee's job description, to use said person's computer, computer network, computer program, computer software, computer system, property, or services as those terms are defined in this section;

(c) "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device;

(d) "Computer network" means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers;

(e) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer systems;

(f) "Computer software" means computer programs, procedures, and associated documentation concerned with the operation of a computer system;

(g) "Computer system" means a set of related, connected, or unconnected, computer equipment, devices, and software;

(h) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computerized representation thereof;

(i) "Intellectual property" includes data, computer programs, computer software, trade secrets, copyrighted materials and confidential or proprietary information in any form or medium when such is stored in, produced by, or intended for use or storage with or in a computer, a computer system, or a computer network;

(j) "Person" shall include any individual, partnership, association, corporation, or joint venture;
(k) "Proper means" includes;
(i) Discovery by independent invention;
(ii) Discovery by "reverse engineering;" that is, by starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must be by lawful means;
(iii) Discovery under license or authority of the owner;
(iv) Observation of the property in public use or on public display; or
(v) Discovery in published literature;
(l) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value;
(m) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

Comment: As mentioned previously, although there is no model computer crime statute, there are certain areas in which the various state acts are similar. The definitional section proposed here is one of those,[44] as most of these definitions are extremely similar in nearly all states with computer-related crime laws.[45] Generally, these definitions are both plain enough for members of the legal profession to understand, and technical enough to satisfy the demands of the

---

44. *See, e.g.*, COLO. REV. STAT. § 18-5.5-101 (1980).

45. The terms "intellectual property" and "proper means" are somewhat different, not so much because the definitions provided here are variant ones, but because they are only included in two of the other state codes. *See* LA. REV. STAT. ANN. § 73.2 (West 1986); MISS. CODE ANN. § 97-45-9 (Supp. 1987). The reason for the inclusion of these terms in this glossary will become apparent when the proposed section of the code dealing with offenses against intellectual property, W. VA. CODE § 61-3C-6, is discussed.

It should also be noted that a Louisiana state court recently found a portion of that state's computer crime act unconstitutional due to the vague definition of the term "access." State of Louisiana v. Azar, No. K88-273 (La. Ct. App. 3rd Cir. Sept. 12, 1988) (WESTLAW, 1988 LA 94929). The Louisiana definition is very similar to the one given here. The court based its holding on the determination that a person could "access" a computer within the definition without being aware that such an "access" had occurred. The court argued that the failure to require knowledge on the part of the user rendered the definitionunconstitutionally vague.

This approach seems to be unrealistic however. It is hard to imagine many typical instances in which a person has "accessed" a computer and been unaware of the occurrence. Furthermore, it is even more difficult to conceive of a computer criminal who does not realize that a computer has been "accessed." There is nothing illegal in the mere "accessing" of a computer; it only becomes such when connected with a bad intent as the proscriptive sections of the Louisiana statute, and the act proposed by this note, plainly require. Thus, the Louisiana court seemed to ignore the practical realities of this type of crime by relying on the miniscule chance that someone could actually commit a computer crime without even having realized it.

computer field,[46] with the only relevant difference being the definition of "computer."[47]

The definition of "computer" given here differs from the majority of state statutes.[48] The overly broad definition of "computer" has been the subject for criticism of many state computer crime acts.[49] The definition adopted here, while being broad enough to cover everything that is considered to be a computer at this point in our technology, also rules out the inclusion of such items as calculators or automated typewriters[50] and thus avoids the possibility of any ridiculous charges against a person for the unauthorized use of such devices. In addition, by including terms such as "electrochemical" it allows for the rapid technological advances that are continually being made, adding future flexibility to the definition.

B. Computer Fraud, Computer Trespass, and Offense Against Intellectual Property

> § 61-3C-4. Computer fraud.
> Whoever knowingly and willfully, directly or indirectly accesses or causes to be accessed any computer, computer system, or computer network 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 shall be guilty of computer fraud and shall be subject to the penalties set forth in § 61-3C-7.

---

46. Note, *Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act*, 27 WM. & MARY L. REV. 783, 791 (1986).

47. This definition of "computer" is borrowed from the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, *supra* note 24, in which the term "computer" was defined "as specifically as possible in order to avoid future attacks on the statute for vagueness." M. ROSTOKER & R. RINES, *supra* note 9, at 346.

48. A large number of the states have based their definition of "computer" on the one used in the proposed Federal Computer Systems Protections Act of 1979, *supra* note 41. Hawaii's use of that definition reads:

> "Computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a computer system or computer network.

See, e.g., HAW. REV. STAT. § 708-890 (1985). This definition has been criticized for being overly broad. *See* Note, *supra* note 18, at 768.

49. *See* Note, *supra* note 46, at 794.

50. This definition avoids the criticism leveled against many other state statute definitions of "computer" which may include calculators and similar devices within their coverage. *See id.* at 794.

Comment: This section reflects the stated legislative purpose of the act.[51] It prohibits the use of a computer to do that which is generally illegal under existing law but which might be difficult to prosecute absent this statute. As the plain language of this section suggests, it would not be legal for one to devise or execute a fraudulent scheme on or with a computer; nor could one obtain property or services by false pretenses through the aid of a computer. Again, it is obvious that the use of fraud and false pretenses are already criminal acts, but this section clearly makes illegal the use of a computer for these purposes.[52] This section incorporates standard language that is relatively common to those states with computer-related laws.[53] Therefore, there will most certainly be some helpful judicial authority regarding this wording and its legal interpretation and effect.[54]

> § 61-3C-5. Computer trespass.
> Whoever intentionally and without authorization, (1) directly or indirectly accesses, alters, damages, or destroys any computer, computer system, computer network, computer software, computer program or data contained in such computer, computer system, computer program or computer network; or (2) gives or publishes a password, identifying code, personal identification number or other confidential information about a computer, computer system, or computer network shall be guilty of computer trespass and shall be subject to the penalties set forth in § 61-3C-7.

Comment: Most of the first part of this section is covered to some extent by existing law relating to the destruction of property. However, this portion of the act also considers some of the more subtle changes that can be effected inside a computer or its system by various types of computer sabotage and makes such actions punishable offenses.[55] This section addresses the computer "virus" prob-

---

51. This section was originally found in the Federal Computer Systems Protection Act of 1979, *supra* note 41. *See, e.g.*, Sokolik, *supra* note 1, at 378 n.98.

52. However, there is one major difference in that the offense defined by this section could be classified as an "attempt crime." The only thing that need be proven is access to a computer with a certain intent, and not that any sort of property was actually obtained. *See* R. NIMMER, THE LAW OF COMPUTER TECHNOLOGY para. 9.04(2) (1985).

53. *See, e.g.*, N.M. STAT. ANN. 30-16A-3 (1988).

54. An almost identical section of the Tennessee Computer Crimes Act was recently upheld against attack as being unconstitutionally vague and overbroad in an as yet unreported decision. State of Tennessee v. Joyner, No. 59 (Tenn. Crim. App. Sept. 30, 1987)(WESTLAW 1987 TN 48853).

55. This section was originally found in the Federal Computer Systems Protection Act of 1979, *supra* note 41.

lem that has recently plagued the field and expressly outlaws this particularly dangerous and infectious practice that might otherwise fall between the cracks of existing law.[56] It also proscribes the accessing of a computer or its system when one is not authorized to do so. Such "hacking" has, of course, been the prime objective of some computer enthusiasts.[57] Further, it should be noted that the first sentence of this section requires an intentional act for prosecution. This protects those who might innocently stumble into a system or data which they should not have accessed. The requirement of intent allows such unintentional acts to go unpunished.

While the first portion of this type of computer trespass statute is relatively common among the various state codes,[58] the second part is not. Language making it illegal to reveal passwords or codes without authorization is present in only one other state act;[59] yet it significantly enhances the quality of the statute. Currently, some, though not a large number, of electronic "bulletin boards" are used to disclose unauthorized passwords and access codes. This section prohibits such a practice, thus promoting computer security. And since it requires an intentional act, this provision will not put the operator of such a bulletin board in jeopardy unless he knowingly allows such disclosures to continue or refuses to remove unauthorized codes when found on his board.[60] This proscription plainly is not limited to "bulletin board" abuse alone, but applies to any means of public dissemination of a private code. Consequently, it could be a strong deterrent to the handing out of such information and could aid considerably those fighting breaches of computer security, breaches that are further compounded by unauthorized users possessing valid access codes.

§ 61-3C-6. Offense against intellectual property.

(1) An offense against intellectual property is the intentional (a) destruction, in-

56. See Elmer-DeWitt, *supra* note 12, for a thorough explanation of the computer "virus" problem.

57. *See generally* A. BEQUAI, *supra* note 2, at 29-43.

58. *See, e.g.*, GA. CODE ANN. § 16-9-93(b) (1984).

59. 18 PA. CONS. STAT. ANN. § 3933(a)(3) (Purdon Supp. 1988).

60. *See* Soma, Smith, & Sprague, *supra* note 5, at 605; Note, *Computer Bulletin Board Operator Liability for User Misuse*, 54 FORDHAM L. REV. 439 (1985).

sertion or modification, without authorization, of intellectual property; or (b) disclosure, use, copying, taking or accessing, without authorization, of intellectual property.

(2) Whoever commits an offense against intellectual property shall be subject to the penalties set forth in 61-3C-7.

(3) The provisions of this section shall not apply to the disclosure, use, copying, taking or accessing by proper means as defined in this article.

Comment: The preceding two sections deal generally with the use of a computer to commit fraud, and the illegal access of or damage to a computer or its system. Such measures are the extent of protection afforded by many state computer crime acts. However, the copying of software and data are important areas of computer crime often left untouched by this kind of legislation although the potential for abuse is equally great. The section above is specifically directed at such acts.[61]

Under existing law, nothing tangible is actually taken when something is copied without permission from a computer's memory.[62] Depending upon the method employed (and the quantity of material being copied), the only adverse result might be an inability to access the material for a brief period of time.[63] Thus, under conventional law, it is doubtful that a crime has been committed.

This section clearly defines such copying as criminal. While many computer programs are copyrighted, and thus protected by copyright laws, this portion of the act will protect programs not yet copyrighted or any other work product or data stored within a computer's memory while providing an extra measure of protection for copyrighted materials. Even though its provisions against destruction and modification of intellectual property duplicate somewhat the preceding computer trespass section, the problem posed by the copying of materials requires a separate sanction. Further, including a copying proscription in the trespass section would not address as plainly the complicated questions involved as would this separate

61. The section of code that this portion of the proposed statute is borrowed from is found in only two states. MISS. CODE ANN. § 97-45-9 (Supp. 1987); LA. REV. STAT. ANN. § 14:73.2 (West 1986).

62. M. ROSTOKER & R. RINES, *supra* note 9, at 341.

63. For a good description of how this would be performed, see Note, *supra* note 46, at 823 n.202.

provision which prohibits the copying of such intangible property residing in a computer's memory banks. This section also makes an allowance for the discovery of such information by "proper means," which is more fair and reasonable than an outright proscription against copying. By permitting such activity, there is no repression of creativity and no fear that an innocent computer buff attempting to dissect and duplicate a computer program obtained by lawful means will be punished for doing so. Therefore, a more complete result is obtained under this specific section. Directed exclusively at the protection of intellectual property, this provision would most likely have a deterrent effect more important than its actual use as a tool for prosecution.

This section would also be effective against computer "viruses." Unlike the computer trespass provision, it prohibits the unauthorized insertion of those destructive programs. While the trespass section will safeguard against the accessing or alteration of a particular computer system or program, this section can more effectively be used against those who unleash a "virus" that automatically inserts itself into any computer system it contacts without further programmer control. Such a law would provide a wider range of protection against the creation and intentional release of computer "viruses" than could either code section standing alone.

In sum, the major difference between the computer trespass section of the act and this section is that the former is aimed chiefly at protecting the system itself while the latter is directed more at the protection of what is actually contained within by the system. Though these two provisions overlap, both are necessary for completely safeguarding against the many possible forms of computer crime.

C. Penalties, Presumptions, and Venue

§ 61-3C-7. Penalties.
For the purposes of this section:
(1) The value of property or computer services shall be (a) the market value of the property or computer services at the time of the violation; or (b) if the property or computer services are unrecoverable, damaged, or destroyed as a result of a violation of W. Va. Code § 61-3C-4, § 61-3C-5, or § 61-3C-6 the cost of re-

producing or replacing the property or computer services at the time of the violation.
(2) Amounts included in violations of W. Va. Code § 61-3C-4, § 61-3C-5, or § 61-3C-6 committed pursuant to one scheme or course of conduct, whether from the same person or several persons, may be aggregated in determining the grade of the offense.
(3) When the value of the property or computer services or damage thereto cannot be satisfactorily ascertained, the value shall be deemed to be $250.
(4) A person who violates this act, if the violation involves $250 or less, is guilty of a misdemeanor. If the violation involves more than $250, the person is guilty of a felony, punishable by imprisonment for not more than 10 years, or a fine of not more than $5,000, or both.

Comment: This section of the code is not as complicated as it might first appear.[64] If the value of the property or services damaged by a violation of this article is greater than $250, then a felony has been committed; if the amount is less than or equal to $250, it is a misdemeanor. The value is to be determined from the market value of the property or service at the time of the crime. If the property has been destroyed, the value is equivalent to the cost of reproduction. Also, the total amount of damage done by several persons can be aggregated, if the actions are all part of one scheme, to determine whether a felony has been committed. Finally, if the value is indeterminable, then it is deemed to be a misdemeanor amount.

As for the actual penalties, the possible ten-year sentence for a conviction under this act, though severe, is appropriate. Certainly when the typical amount involved in these kinds of crime is considered, it can hardly be thought of as too harsh a maximum sentence. In some states, any violation of this type of law is a felony without regard to the amount of damage actually caused.[65] But it is more equitable, and consistent with notions of culpability, to base the grade of the offense on the value of the harm done. Such a scale will also protect against the imposition of severe penalties on younger computer users who are sometimes prone to breaking into protected systems. Even though such activity is more than a nuisance, if there is no actual damage done, then there should not be a harsh sanction. Finally, in order to serve a deterrence function,

64. This section, with some minor additions, is based on N.H. REV. STAT. ANN. § 638:18(V) (1986).

65. Note, *supra* note 18, at 769.

there must be a severe penalty for those who might contemplate committing a more serious type of computer crime.[66] Overall, basing the grade of the offense and the resulting penalty on the value of the damage done is the most preferable way to punish this kind of white-collar crime.

§ 61-3C-8. Rebuttable presumption; without authority.
In the event that a person accesses or causes to be accessed a computer, which access requires a confidential or proprietary code which has not been issued to or authorized for use by that person, a rebuttable presumption exists that the computer was accessed without the authorization of its owner or in excess of the authority granted.

§ 61-3C-9. Computer printouts as evidence.
In a prosecution under W. Va. Code § 61-3C-4, § 61-3C-5, or § 61-3C-6 computer printouts shall be competent evidence of any computer software, program, or data contained in or taken from a computer, computer system, or computer network.

Comment: These two sections are directed at aiding the prosecution of those accused of computer crime. Each of these provisions is found in only one other state act,[67] though both are effective means of assisting prosecution and thus deserve inclusion in the proposed statute. The first section, § 61-3C-8, shifts the burden of proof to the accused to show that he had the requisite authority to use a computer for which he had not been issued the required access code. While this creates a rebuttable presumption of fact that such a user is without authority, it should be noted that a violation of one of the various provisions of this statute requires an intentional, unauthorized act. The mere presumption of a lack of authority is insufficient by itself to hold one guilty of any computer crime. Thus, while this section aids prosecution, it does not infringe upon any right of an individual charged since there cannot be a conviction unless the accused has committed an intentional (v. merely unauthorized) violation of these provisions. Further, such a provision might encourage computer owners to take security measures since accurate record-keeping of authorized users will simplify prosecu-

66. *See generally* A. BEQUAI, *supra* note 2, at 61-76 (noting the movement of organized crime into the computer crime field).

67. Proposed § 61-3C-8 is based on ILL. ANN. STAT. ch. 38, a¶a 16D-7 (Smith-Hurd Supp. 1988). Section 61-3C-9 is taken from MO. ANN. STAT. § 569.094 (Vernon Supp. 1988).

tions for breaches of computer systems, and, in turn, further discourage potential white-collar criminals.

The second section, § 61-3C-9, is also designed to eliminate doubt and aid prosecution by stating in an unqualified manner that computer printouts are competent evidence as to what is or is not in a computer or its system. There is little doubt that such printouts are admissible for this purpose. However, depending upon the posture of the defense in any one particular case, the introduction of such printouts may require the time-consuming laying of foundation. By clearly delineating their admissibility for this purpose, much delay can be avoided. This section facilitates prosecution since any action under this act will probably require the introduction of computer printouts. Both of these provisions are merely designed to make the job of prosecuting someone under this article easier, since any case involving computers has the potential to become extremely complicated even to those with some expertise in the field.[68]

§ 61-3C-10. Venue.
For the purpose of venue under this article, any violation of this article shall be considered to have been committed in any county:
(1) In which any act was performed in furtherance of any course of conduct which violated this article;
(2) In which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, data or other material or objects which were used in furtherance of the violation;
(3) From which, to which, or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication;
(4) In which any computer, computer system, or computer network is an object or an instrument of the violation is located at the time of the alleged violation.

§ 61-3C-11. Article not exclusive.
The provisions of this article shall not be construed to preclude the applicability of any other provision of the criminal law of this State which presently applies or may in the future apply to any transaction or course of conduct which violates this article, unless such provision is clearly inconsistent with the terms of this article.

68. *See* A. BEQUAI, *supra* note 2, at 118-120 (noting the lack of computer training among those charged with the enforcement of our laws).

Comment: Venue under § 61-3C-10 is very broad.[69] It would even be proper in a county through which communication by microwaves passed between the criminal and the computer system. Other than the microwave provision, however, this is a standard venue provision similar to other state acts. The other section, § 61-3C-11, provides that all other laws of the state are applicable to any matter addressed by this statute unless inconsistent with one of its provisions.[70]

D. Civil Actions

> § 61-3C-12. Civil actions.
> (1) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of the suit. Without limiting the generality of the term, "damages" shall include loss of profits.
> (2) At the request of any party to an action brought pursuant to this section, the court, in its discretion, may conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer system, computer network, computer program, computer software, and data involved in order to prevent possible recurrence of the same or a similar act by another person and to protect trade secrets of any party.
> (3) The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.
> (4) A civil action under this section must be commenced before the expiration of the time period prescribed in W. Va. Code § 55-2-12.

Comment: This provision explicitly creates a private cause of action for the violation of this article.[71] It allows for the actual damages, including the costs of the suit. Any right of action under this section is limited to a two-year statute of limitations under W. Va. Code § 55-2-12. This section also specifically does not exclude any other remedy an individual might have under other applicable law.

Also of importance is the unique security provision contained within this section. At the request of any party to a suit, the court, in its discretion, can take action to assurethat the security of any computer system is not breached during the legal proceedings. This helps to ensure that a similar crime will not follow. This will also

---

69. This section can be found in several state codes. *See, e.g.*, ARK. STAT. ANN. § 5-41-105 (Supp. 1987).

70. *See, e.g.*, VA. CODE ANN. § 18.2-152.11 (1988).

71. This section is found in several state codes. *See, e.g.*, VA. CODE ANN. § 18.2-152.12 (1988).

substantially encourage the reporting of such crimes since businesses might be willing to enforce their rights in court if they can safeguard the security of their computer systems at the same time.

E. Severability and Assistance of Attorney General

§ 61-3C-13. Severability.
If any provision or clause of this article or application thereof to any person or circumstance is held to be invalid, such invalidity shall not affect other provisions or applications of this article which can be given effect without the invalid provision or application, and to this end the provisions of this article are declared to be severable.

§ 61-3C-14. Assistance of Attorney General.
If requested to do so by a prosecuting attorney, the Attorney General may assist the prosecuting attorney in the investigation or prosecution of an offense under this article or any other offense involving the use of a computer.

Comment: The first of these two sections is a very standard severability clause.[72] It provides that if some part of this act is found to be invalid, the rest of the statute is still valid to the extent that it did not depend on the invalidated section. The second provision permits the Attorney General, upon request, to step in and assist a county prosecutor.[73] This might be useful since any computer crime prosecution could quickly exceed the technical knowledge of the average person, and the help of someone with some expertise in the field could be invaluable. The state government could also provide additional resources to any particular prosecution, and, in instances of computer crime extending across county or state borders, the assistance of the Attorney General might be a necessity.

VI. CONCLUSION

While the vast majority of states have at least proposed some answers to the problem of computer crime, West Virginia has remained silent despite the high growth rate of such crime and the difficulties inherent in its prosecution under the existing law of the state. Though state computer crime acts have not gone without criticism, they are the most effective statutory method of addressing

72. This section is rather standardized. *See, e.g.*, VA. CODE ANN. § 18.2-152.13 (1988).
73. This section is borrowed from ARK. STAT. ANN. § 5-41-108 (Supp. 1987).

this problem. The proposed West Virginia Computer Crimes Act is a synthesis of the best aspects of existing state acts adapted and supplemented for use here. This approach will allow the courts of this state an opportunity to utilize interpretive case law from other jurisdictions concerning the same, or similar, statutory sections proposed by this note. While it is not imagined that this is a flawless proposal, hopefully it will stimulate debate and serve as a catalyst for the adoption of a comprehensive computer crime act in West Virginia.

Jeffry A. Pritt

(*Editor's note: As of the date of publication of this article, the Regular Session of the 1989 West Virginia Legislature was considering S.B. 92, a proposal for a computer crimes act that, in its amended form, would adopt many of the provisions discussed above.*)

APPENDIX
THE PROPOSED WEST VIRGINIA COMPUTER CRIMES ACT

§ 61-3C-1. Title.

This article shall be known by the short title of "The West Virginia Computer Crimes Act."

§ 61-3C-2. Legislative purpose.

It is found and determined that computer-related crime poses a major problem for business and government; that losses for each incident of computer-related crime are potentially astronomical; that the opportunities for computer-related crime in business and government through the introduction of fraudulent records into a computer system, the unauthorized use of computers, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great; that computer-related crime has a direct effect on state commerce; and that, while various forms of computer crime might possibly be the subject of criminal charges based on other provisions of the law, it is appropriate and desirable that a statute be enacted which deals directly with computer crime.

§ 61-3C-3. Definitions.

The following words when used in this article have the meaning hereinafter ascribed to them, unless the context clearly indicates a different meaning:

(a) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise make use of any resources of, a computer, computer system, or computer network;

(b) "Authorization" means the express consent of a person, which may include an employee's job description, to use said person's computer, computer network, computer program, computer software, computer system, property, or services as those terms are defined in this section;

(c) "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing

logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device;

(d) "Computer network" means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers;

(e) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer systems;

(f) "Computer software" means computer programs, procedures, and associated documentation concerned with the operation of a computer system;

(g) "Computer system" means a set of related, connected, or unconnected, computer equipment, devices, and software;

(h) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computerized representation thereof;

(i) "Intellectual property" includes data, computer programs, computer software, trade secrets, copyrighted materials and confidential or proprietary information in any form or medium when such is stored in, produced by, or intended for use or storage with or in a computer, a computer system, or a computer network;

(j) "Person" shall include any individual, partnership, association, corporation, or joint venture;

(k)"Proper means" includes;

(i) Discovery by independent invention;

(ii) Discovery by "reverse engineering;" that is, by starting with the known product and working backward to find the method

by which it was developed. The acquisition of the known product must be by lawful means;

(iii) Discovery under license or authority of the owner;

(iv) Observation of the property in public use or on public display; or

(v) Discovery in published literature;

(l) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value;

(m) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

§ 61-3C-4. Computer fraud.

Whoever knowingly and willfully, directly or indirectly accesses or causes to be accessed any computer, computer system, or computer network 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 shall be guilty of computer fraud and shall be subject to the penalties set forth in § 61-3C-7.

§ 61-3C-5. Computer trespass.

Whoever intentionally and without authorization, (1) directly or indirectly accesses, alters, damages, or destroys any computer, computer system, computer network, computer software, computer program or data contained in such computer, computer system, computer program or computer network; or (2) gives or publishes a password, identifying code, personal identification number or other confidential information about a computer, computer system, or computer network shall be guilty of computer trespass and shall be subject to the penalties set forth in § 61-3C-7.

§ 61-3C-6. Offense against intellectual property.

(1) An offense against intellectual property is the intentional (a) destruction, insertion or modification, without authorization, of intellectual property; or (b) disclosure, use, copying, taking or accessing, without authorization, of intellectual property.

(2) Whoever commits an offense against intellectual property shall be subject to the penalties set forth in § 61-3C-7.

(3) The provisions of this section shall not apply to the disclosure, use, copying, taking or accessing by proper means as defined in this article.

§ 61-3C-7. Penalties.

For the purposes of this section:

(1) The value of property or computer services shall be (a) the market value of the property or computer services at the time of the violation; or (b) if the property or computer services are unrecoverable, damaged, or destroyed as a result of a violation of W. Va. Code § 61-3C-4, § 61-3C-5, or § 61-3C-6 the cost of reproducing or replacing the property or computer services at the time of the violation.

(2) Amounts included in violations of W. Va. Code § 61-3C-4, § 61-3C-5, or § 61-3C-6 committed pursuant to one scheme or course of conduct, whether from the same person or several persons, may be aggregated in determining the grade of the offense.

(3) When the value of the property or computer services or damage thereto cannot be satisfactorily ascertained, the value shall be deemed to be $250.

(4) A person who violates this act, if the violation involves $250 or less, is guilty of a misdemeanor. If the violation involves more than $250, the person is guilty of a felony, punishable by imprisonment for not more than 10 years, or a fine of not more than $5,000, or both.

§ 61-3C-8. Rebuttable presumption; without authority.

In the event that a person accesses or causes to be accessed a computer, which access requires a confidential or proprietary code which has not been issued to or authorized for use by that person, a rebuttable presumption exists that the computer was accessed without the authorization of its owner or in excess of the authority granted.

§ 61-3C-9. Computer printouts as evidence.

In a prosecution under W. Va. Code § 61-3C-4, § 61-3C-5, or § 61-3C-6 computer printouts shall be competent evidence of any computer software, program, or data contained in or taken from a computer, computer system, or computer network.

§ 61-3C-10. Venue.

For the purpose of venue under this article, any violation of this article shall be considered to have been committed in any county:

(1) In which any act was performed in furtherance of any course of conduct which violated this article;

(2) In which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, data or other material or objects which were used in furtherance of the violation;

(3) From which, to which, or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication;

(4) In which any computer, computer system, or computer network is an object or an instrument of the violation is located at the time of the alleged violation.

§ 61-3C-11. Article not exclusive.

The provisions of this article shall not be construed to preclude the applicability of any other provision of the criminal law of this State which presently applies or may in the future apply to any transaction or course of conduct which violates this article, unless such provision is clearly inconsistent with the terms of this article.

§ 61-3C-12. Civil actions.

(1) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of the suit. Without limiting the generality of the term, "damages" shall include loss of profits.

(2) At the request of any party to an action brought pursuant to this section, the court, in its discretion, may conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer system, computer network, computer program, computer software, and data involved in order to prevent possible recurrence of the same or a similar act by another person and to protect trade secrets of any party.

(3) The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(4) A civil action under this section must be commenced before the expiration of the time period prescribed in W. Va. Code § 55-2-12.

§ 61-3C-13. Severability.

If any provision or clause of this article or application thereof to any person or circumstance is held to be invalid, such invalidity shall not affect other provisions or applications of this article which can be given effect without the invalid provision or application, and to this end the provisions of this article are declared to be severable.

§ 61-3C-14. Assistance of Attorney General.

If requested to do so by a prosecuting attorney, the Attorney General may assist the prosecuting attorney in the investigation or prosecution of an offense under this article or any other offense involving the use of a computer.