University of Richmond Law Review

Volume 19 | Issue 1 Article 5

1984

Virginia's Response to Computer Abuses: An Act in Five Crimes

Daniel R. Burk

Follow this and additional works at: http://scholarship.richmond.edu/lawreview

 Part of the Computer Law Commons, and the Criminal Law Commons

Recommended Citation

Daniel R. Burk, *Virginia's Response to Computer Abuses: An Act in Five Crimes*, 19 U. Rich. L. Rev. 85 (1984).
Available at: http://scholarship.richmond.edu/lawreview/vol19/iss1/5

This Article is brought to you for free and open access by UR Scholarship Repository. It has been accepted for inclusion in University of Richmond Law Review by an authorized editor of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.

VIRGINIA'S RESPONSE TO COMPUTER ABUSES: AN ACT IN FIVE CRIMES*

*Daniel R. Burk***

"GREETINGS PROFESSOR FALKEN"

"Hello"

* * *

"SHALL WE PLAY A GAME?"

"Love to. How about Global Thermonuclear War?"

"WOULDN'T YOU PREFER A GOOD GAME OF CHESS?"[1]

And thus the most romanticized tale of the success of one resourceful teenager began for the viewers of the motion picture *War Games*. The threat depicted in *War Games* has been both rebuked as impossible and highlighted as much closer to the realm of possibility than even the creators of the movie may have surmised. Regardless of the actual possibility of a creative mind breaking through the security of the North America Air Defense Command computer with an auto-dialing modem and the simple password "JOSHUA" the adventures of the curious "hackers" and the singularly-directed criminal have been widely publicized and have captured both the fear and respect of computer owners throughout the country.

This high-technology criminal activity captured the attention of the Virginia legislature in 1984. Virginia, a state which has sought to maintain its historic image, has in recent legislative sessions taken a major and comprehensive step toward addressing the very real threat of computer abuses. The 1984 session of the General

---

* Copyright 1984, 1985 by Daniel R. Burk, all rights reserved.

** Daniel R. Burk is associated with the Washington, D. C. office of Cadwalader, Wickersham & Taft in its computer law division. He drafted the initial version of the Virginia Computer Crimes Act and participated in the legislative process through which the Act was approved. The author wishes to express his appreciation for the assistance provided by S. Miles Dumville, Esquire, of the Richmond office of Thomas & Fiske, P.C., who worked with Mr. Burk in obtaining passage of the Act. An earlier version of this article originally appeared in 3 COMPUTER L. REP. 3 (1984).

1. *War Games*, MGM/UA Entertainment Co., 1983.

Assembly passed the Virginia Computer Crimes Act, which Governor Charles S. Robb signed into law on April 11, 1984. The Act became effective on July 1, 1984.[2] The Act provides unusual solutions to various definitional and procedural issues facing all states which have passed or are considering computer-oriented criminal legislation. The most notable provision creates civil remedies for the injured victim of computer-related crimes in addition to existing civil remedies. Guidance from the Virginia solution to these issues may be attractive to other state legislatures throughout the nation.

This article recalls some of the cases of computer abuses which have been publicized around the country. Next, the article examines the computer-related crimes which have been reviewed by the Virginia Supreme Court. Finally, the Virginia Computer Crimes Act itself will be discussed. This last discussion includes an analysis of the changes that the Act underwent during its review by the General Assembly.

I. Setting the Stage

It was estimated in 1983 that there existed one computer for every 150 children in this country.[3] It has also been estimated that there are as many as 3.5 million personal computers in use, and "[m]arket projections indicate that there will be over seven million personal computers in use within three years. Of these, nearly two million will have the ability to communicate with remote computers."[4] Other estimates suggest that nine million computers are in the nation's offices, schools and homes, and that nine million more are likely to be added every three years.[5]

It is no wonder that computer owners and users, as well as legislators, are concerned about the increasing possibility of computer abuse. Computer users have been forced to spend considerable sums of money to enhance the security of their systems. For example, the press secretary for the Los Angeles County district attorney, Al Albergate, commented: "It's our belief it will cost . . .

2. Va. Code Ann. § 18.2-152.1 through 18.2-152.14 (Cum. Supp. 1984).

3. Myers, *Hacker Debate Continues at Security Conference—Lonely Misfits or Budding Criminals*, Computerworld, Nov. 14, 1983, at 17-18, col. 1.

4. Subcomm. on Crime, House Comm. on the Judiciary (testimony of Peter C. Waal, Vice-President of Marketing and Plans, GTE Telenet, Nov. 10, 1983).

5. Washington Post, May 22, 1984, at 1, col. 2.

agencies and institutions [affected by the activity of a single hacker] hundreds of thousands of dollars to reprogram their systems in order to prevent this [computer abuse] from recurring. . . ."[6] One computer security manager suggested that one percent of a company's annual budget should be spent on data security.[7]

The market is trying to respond to the computer owner's need for additional protection. One insurance company advertisement displays two black-gloved hands typing on a computer terminal with the title on the ad reading: "Computer crime. You can't prevent it, so you'd better be insured against it."[8] Similarly, an advertisement for a vendor of a physical security system depicts a western-style holster wrapped around the corner of a computer display screen. The caption reads: "You've come a long way, Jesse James."[9] But insurance does little to deter the would-be offender, and while the sophistication of security devices is increasing, such improvements may do nothing more than challenge the creative hacker.

Only a few years ago, listing the cases of reported "computer crimes" would have been a simple task. Today, however, the list is so long that generalized categories are needed to understand the nature of the abuses.[10] These categories include situations where:

1. The computer data is the object of the crime. Computerized information is viewed or changed by the offender causing some harm or invasion of privacy. Examples of this category include three San Diego high school students who deleted grades and altered the homework of other students[11] as well as four municipal court employees who were fired for allegedly accepting bribes to alter traffic citation and arrest warrant status information main-

6. Hafner, *Felony Charges Filed Against Alleged Hacker*, Computerworld, Nov. 14, 1983, at 15, col. 1.

7. *D.P. Crime: Where There's A Will, There's A Way*, Computerworld, Dec. 26, 1983/Jan. 2, 1984, at 53, col. 1.

8. Computerworld, Nov. 28, 1983, at 18 (advertisement for Shand, Morahan & Co., Inc., Evanston, Ill.).

9. *Id.* at 30 (advertisement for LeeMAH, San Francisco, Cal.).

10. For various categorizations, see, e.g., Note, *A Suggested Legislative Approach to the Problem of Computer Crime*, 38 WASH. & LEE L. REV. 1173, 1175 (1981); Parker & Nycum, *Computer Crime*, 27 COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY (ACM) 313 (1984).

11. 2 COMPUTER L. REP. 1029 (1984).

tained by a computer.[12] Other instances involve computerized account information at the Bank of America which was allegedly adjusted to show sufficient balances to permit the offender to withdraw large sums of cash from this account.[13] Account information maintained by a computer at Merrill, Lynch, Pierce, Fenner and Smith, Inc. was also allegedly revised to show that an account was ready for disbursement even though the checks funding the account had not in fact cleared.[14] Still another example of this category involved employees of a law firm, in conjunction with an unemployed broker, who allegedly used a computer to access the law firm's confidential files in order to obtain inside information regarding the firm's clients. These employees then traded in the stock market based on that inside information.[15]

2. The physical computer is the object of the crime. For example, the computer may be stolen or may be a target for physical violence because of the computer's importance to the operations of its owner.

3. The computer's processing capabilities are the object of the crime because either the processing time or storage functions are valuable. For example, a police department computer was used by a part-time policeman to check employment records for the policeman's full-time employer.[16]

4. The computer is the central hub of many users or functions and the offender participates in that hub, intending to create a nuisance. Examples of this category include the "414's," self-titled in honor of their Milwaukee telephone area code, who invaded several computer facilities, including New York's Sloan-Kettering Cancer Center where life-saving cancer treatment data stored on the computer was altered.[17] Another instance involved a "computer hobbyist" who attempted to "crash" a computer at Columbia University and caused thousands of dollars of damage and the loss of large amounts of data.[18] Other examples include a programmer who inserted a system-wide nuisance which randomly printed

12. Computerworld, Nov. 8, 1982, at 9, col. 1.
13. Computerworld, Dec. 20, 1982, at 5, col. 1.
14. *Id.*
15. Computerworld, Apr. 9, 1984, at 33, col. 1.
16. N.Y. Times, Sept. 18, 1983, § 1, at 1, col. 1. For a similar story, see Computerworld, Feb. 20, 1984, at 8, col. 4.
17. *See* NEWSWEEK Sept. 5, 1983, at 42-48; *Id.* Aug. 29, 1983, at 45-49.
18. N.Y. Times, Sept. 18, 1983, § 1, at 1, 42, col. 1.

"cookie" on a user's screen until the word "cookie" was entered by the user[19]and a nineteen-year-old University of California at Los Angeles student who allegedly broke into two hundred accounts at fourteen separate sites.[20]

II. THE OVERTURE

The cases reviewed by the Supreme Court of Virginia regarding improper uses of a computer system have been few. In 1977, the court concluded that the unauthorized use of computer time and services could not form the basis of a conviction for larceny because these were not "goods or chattels."[21]

In response to that decision, the Virginia General Assembly in 1978 passed a simple act containing one sentence which addressed computer time and services: "Computer time or services or data processing services or information or data stored in connection therewith is hereby defined to be property which may be the subject of larceny . . . , or embezzlement . . . , or false pretenses . . . ."[22]

In 1983, the Virginia Supreme Court was asked to determine whether taking computer printouts from an employer constituted embezzlement. Citing the new Virginia Code section, the court held that these printouts represented computer information and data and were therefore proper subjects of prosecution.[23]

In late 1983, the Virginia legislature reviewed three bills designed to expand the coverage of Virginia Code section 18.2-98.1. The first bill, House Bill 6, was prefiled by Delegates Clifton A. Woodrum and Richard Cranwell. This bill defined "computer," "computer medium," "use of a computer," and "property." The bill also defined three substantive crimes: use of a computer with fraudulent intent resulting in damages, intentional use resulting in damage, and unauthorized use. Levels of penalties ranged from a Class 4 felony, punishable by two to ten years imprisonment, to a Class 1 misdemeanor, punishable by not more than twelve months in jail and/or a $1000 fine.

---

19. *Beware: Hackers at Play*, NEWSWEEK, Sept. 5, 1983, at 42, 45.
20. Hafner, *supra* note 6.
21. Lund v. Commonwealth, 217 Va. 688, 691-92, 232 S.E.2d 745, 748 (1977).
22. VA. CODE ANN. § 18.2-98.1 (Repl. Vol. 1982) (repealed 1984).
23. Evans v. Commonwealth, 226 Va. 292, 297, 308 S.E.2d 126, 129 (1983).

However, there were several problems with House Bill 6. First, it did not define the term "intentional use" and did not address the issue of whether a crime had been committed when the actor knew what he was doing but thought he had permission to do it. Second, the bill excluded hand-held calculators, automated typewriters, and any computer "designed and manufactured for, and which is used exclusively for, routine personal, family, or household purposes and which is not used to access, to communicate with, or to manipulate any other computer." The purpose of this limitation was to prevent prosecution of such insignificant acts as a child's use of his neighbor's computer to play games, but the limitation placed too heavy a burden on the prosecution to prove that the computer involved was actually manufactured or used for a business purpose. In addition, the bill did not clearly define the terms "property" and "computer medium." The definition of property, when referring to computerized information, was information contained on a computer medium, but the definition of "medium" included only the electronics by which data is communicated to a computer. Thus, it was unclear whether information stored in the computer's main memory or on disk or tape would fall within the definition of "property." Finally, although the definition of property referred to data, the bill failed to define the term "data." Whereas a computer professional may have a broad definition of data, the public's perception of data is limited to those numbers and characters which are manipulated by a computer program.

A second proposed bill, House Bill 289, tracked House Bill 6 very closely, but limited its coverage to acts which caused "damage to the property of the Commonwealth or of any state-insured institution," or which affected the use of a computer owned by the state or a state-insured institution. All limitations found in House Bill 6 were also present in House Bill 289, and because of its focus on the state and state-insured institutions, the latter bill did little to benefit the majority of the business community.

Finally, Senate Bill 347 was sponsored by Senator Clive DuVal and was referred to the Senate Committee for Courts of Justice. Like the other two bills, this bill itemized three proscribed activities and levels of intent. However, all proscribed activities were punished with the same penalty: a Class 1 misdemeanor. This was a definite shortcoming of the bill because a user's intentions may make the impact of the crime significantly different, and the associated punishments should recognize these differences.

From discussions among members of the legislature and various representatives from the business community, it became clear that a proposal which either modified or added to the existing struction of Virginia Code section 18.2-98.1 would be complicated. Accordingly, a totally revised act addressing the deficiencies of the existing section 18.2-98.1 was created. Several goals were identified prior to drafting.

First, the act should not only incorporate the best provisions of existing legislation in other states, but should also create a structure which might serve as a uniform computer crimes act on a nationwide basis. Such uniformity would simplify prosecution and defense in each state since guidance could be obtained from rulings in other states.

Second, the legislation should recognize that computer crime is difficult to detect, and that prosecutions may be difficult to obtain. It has been estimated that only one percent of all computer-related crimes is detected. Of those detected, only twenty percent are reported and approximately only one percent of those reported are actually prosecuted.[24] The detection process is hampered by the sheer number of possible sources of access, particularly when a large computer network is involved, by the ease with which computer time can be used without affecting other users, and by the fact that computer data can be altered without leaving a trail.

Prosecution is often hampered by a lack of technical knowledge of computers on the part of judges, juries, and attorneys. Furthermore, prosecution is also impaired if a computer owner fails to cooperate with the authorities because he is concerned about the repercussions of the case. Wide-spread publicity about the crime may encourage repetition, particularly if the method of access is made public through trial, and publicity may also discourage legitimate users from trusting the integrity of the computer system.

Third, the legislation should treat the proscribed activities as *new* crimes rather than as existing crimes. A new article of the Virginia Code dealing only with computer crimes would prevent lawyers and judges from trying to draw too many strained analogies from existing legislation and case law.

---

24. August, *Turning the Computer Into A Criminal*, 10 BARRISTER 12, 14 (Fall 1983) (quoting testimony of Senator Joseph Biden before the Subcomm. on Criminal Laws and Procedure of the Senate Comm. on the Judiciary).

Fourth, criminal fines set forth in the act should not be so financially debilitating for the criminal that the computer owner is unable to recover his actual damages in any future civil suit. By comparison, the various federal proposals do not provide for civil remedies,[25] but such remedies might be ineffective anyway since stiff fines accompany a successful prosecution under the federal acts.

Finally, wherever possible, encouragement should be given to computer owners to document those users having authority to use the system and those persons who have never had such authority or who may have had their authority terminated. Such documentation would negate the defense that the unauthorized use had been made without knowledge of the lack of authority.

With these goals in mind, a new bill was drafted with the assistance of Delegate Woodrum, one of the sponsors of House Bill 6, and upon completion, the revised bill was substituted for the original House Bill 6. The bill was submitted for hearings before the House Courts of Justice Committee, and after obtaining that Committee's approval, the bill was reported to the full House where it passed by a 98 to 2 vote.[26]

Noting the success of the Act in the House, Senator DuVal, patron of Senate Bill 347, agreed to substitute the House measure for the Senate bill. The bill was not revised at all by the Senate Committee for Courts of Justice, and it was passed by the Senate by a 38 to 1 vote.[27]

The Act, as adopted, has fourteen new sections which are located in Virginia Code sections 18.2-152.1 through 18.2-152.14. The final legislation also repeals section 18.2-98.1 since the activity proscribed in the older legislation is intended to be covered by the new legislation.

---

25. *See, e.g.*, 18 U.S.C. § 1029 (1984); H.R. 1092, 98th Cong., 1st Sess. (1984).

26. H.B. 6, Va. Gen. Assembly of 1984, House Journal 791.

27. S.B. 347, Va. Gen. Assembly of 1984, Senate Journal 379-80.

III. The Play's the Thing[28]

A. *Structure*

The Virginia Computer Crimes Act, begins with an extensive set of definitions.[29] The Act specifies the elements of five new crimes not presently found in Virginia's criminal code[30] and addresses the procedural issues associated with criminal prosecutions under the new Act.[31] The Act also provides non-exclusive civil relief for the party injured as a result of the crime.[32] This section is unique as compared with most other states' computer crime acts.[33]

The usual severability provision is included,[34] and the Act concludes with a provision permitting a conviction for forgery where data stored on a computer is revised.[35]

B. *Definitions*

The Act defines thirteen words or phrases.[36] Although several of these definitions originate in the legislation of other states,[37] others were needed because of the original structure proposed for Virginia.

The definition of computer[38] is intentionally broad so that the language will apply to technology which appears after the Act is in effect. For example, "organic device" was included because of the developing technology of biological memory which may have greater capability than the current limitation of two states: "yes" or "no" ("1" or "0"). The definition of a computer was also in-

---

28. Shakespeare, Hamlet, Act II, Scene ii.

29. *See infra* notes 36-57 and accompanying text.

30. *See infra* notes 58-70 and accompanying text.

31. *See infra* notes 71-76 and accompanying text.

32. *See infra* notes 77-85 and accompanying text.

33. The word "unique" is used guardedly since both California (1984 Laws, Chapter 949) and Connecticut (Public Act 84-206) have recently legislated similar civil relief. At present, the Massachusetts legislature is considering a civil remedy.

34. *See infra* note 86 and accompanying text.

35. *See infra* note 87 and accompanying text.

36. Va. Code Ann. § 18.2-152.2 (Cum. Supp. 1984).

37. For example, the definition of "computer software" as contained in Va. Code Ann. § 18.2-152.2 (Cum. Supp. 1984) is taken largely from Ariz. Rev. Stat. Ann. § 13-2301 (1978). Virginia's definition of "financial instrument" almost mirrors Cal. Penal Code § 502(a)(6) (West Supp. 1984). "Computer network" can also be found in Fla. Stat. Ann. § 815.03(6) (West Supp. 1984), and a portion of the definition of "computer program" was borrowed from Ga. Code Ann. § 16.9-92(4) (1984).

38. Va. Code Ann. § 18.2-152.2 (Cum. Supp. 1984).

tended to include all peripheral devices, such as monitoring devices and controlled relays.

Computer data[39] is intended to include all information of *any* type which might be stored in a computer. Both the object and source code formats of programs are included since human and/or machine recognition is irrelevant.

Computer network is defined as any combination of computers and peripherals and their interconnections. In the process of editing the Act, the phrase "computer network" was inadvertently left out of the five sections delineating separate new computer crimes.[40] This omission should not create any difficulty because it is highly likely that a network which is accessed will not be the end target of any criminal activity. As soon as any of the computers comprising any of the nodes of the network is accessed, the defined crimes have been committed, assuming all other required elements of the crimes are met.[41]

It should be noted that in legislation of other states, computer operations[42] was often included as part of the definition of computer. Because the term "use of a computer" includes causing the computer to perform computer operations,[43] a separate definition seemed expedient.

Computer program[44] is defined purely as a subset of computer data.[45] The definition was included to permit the legislature to later consider enacting provisions concerning prevention of improper copying of programs.

The definition of computer services[46] came from the language of the previous law, section 18.2-98.1. The adoption of this language was intended to allow future court cases to use the decision in *Evans v. Commonwealth*[47] as precedent if the same fact situation occurs and a definition of services would otherwise be unclear.

---

39. *Id.*
40. *Id.* §§ 18.2-152.3 to -152.7 (Cum. Supp. 1984).
41. The 1985 General Assembly should, in all likelihood, make the necessary technical amendments.
42. VA. CODE ANN. § 18.2-152.2 (Cum. Supp. 1984).
43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.*
47. 226 Va. 292, 308 S.E.2d 120 (1983). *See supra* note 23 and accompanying text.

Computer software[48] is also a subset of "computer data" if it is stored on a computer. Otherwise, it would include printed materials which aid in the operation of computer programs. Software, and in particular documentation, is of extreme importance to a computer installation, and, if contained in the computer, might be modified in an extremely detrimental way without leaving any trace to alert the owner of the computer.

Financial instrument[49] is defined so that automated teller machine transactions and the wire transfers are protected by this Act. It is possible that the guidance suggested by the legislature in this definition will prompt Virginia courts to recognize that a financial instrument for U.C.C. purposes can include a computer representation of an instrument.

The definition of owner[50] is included so that it is clear that protection and civil remedies will be available for any operator of a computer or licensee of software regardless of whether title to the equipment or data is held by the owner. The Act also uses an all-inclusive definition of person, including partnerships, associations, corporations and joint ventures.[51]

Property[52] is defined broadly so that distinctions between realty and personalty, and between tangible and intangible property, would not be considered relevant. Also, in response to the decision in *Lund v. Commonwealth*,[53] the definition of property includes computer services.

Use of a computer is defined to include some actions which would not normally be associated with the word. For example, causing or attempting to cause a computer to stop performing computer operations is a use.[54] Also, denying the use of a computer to another user is a use and is similarly proscribed. Further, having another person put false information into a computer is a use.

The phrase "without authority,"[55] in reference to using a computer, was explained in detail in order to clarify to owners and users the responsibilities each had when determining rights to use

48. VA. CODE ANN. § 18.2-152.2 (Cum. Supp. 1984).
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. 217 Va. 688, 232 S.E.2d 743 (1977). *See supra* notes 21-22 and accompanying text.
54. *See* VA. CODE ANN. § 18.2-152.2 (Cum. Supp. 1984).
55. *Id.*

a computer. In its original form, the definition read:

> A person is "without authority" when he has no right or authority and no reasonable grounds to believe that he has such authority. A person may be using a computer or computer network without authority even when he has the right to use the computer or computer network in some other manner or has the right to use or gain access to the same computer data or computer programs for another purpose which is authorized.[56]

The House Committee substantially modified the definition. The Committee interpreted the phrase dealing with "no reasonable grounds to believe that he has such authority" as creating an affirmative burden of proof on the defendant.[57] As a practical matter, it is likely that the prosecution would present a minimum amount of evidence to establish absence of authority unless the defendant were able to seriously call this evidence into doubt. In such a case, the defendant would have to provide a minimum amount of evidence to show his reasonable grounds, and the prosecution would then have to show beyond a reasonable doubt that no reasonable ground existed upon which to base relief.

The House amendment removed the availability of an explicit defense of reasonable grounds. In all probability, however, the defense of reasonable grounds will go to the general question of intent to commit the crime. The remainder of the House amendments to this definition simplifies what the Committee perceived as cumbersome language.

C. *New Crimes*

The Act defines five new crimes not found elsewhere in the Virginia Code.

1. Computer Fraud

Computer fraud[58] is committed where a computer is used without authority to obtain property or services by false pretenses, to embezzle or commit larceny, or to convert the property of another. Punishment under this crime is determined on the basis of the

56. Draft proposal of Virginia Computer Crimes Act's definition of "without authority."
57. *Id.*
58. VA. CODE ANN. § 18.2-152.3 (Cum. Supp. 1984).

value of the property or services actually obtained. If the value is $200 or greater, punishment is as a Class 5 felony (imprisonment for between one and ten years or a maximum of twelve months in jail and/or a $1000 fine). Otherwise, the crime is punished as a Class 1 misdemeanor.

This division of punishment based on value was not in the original proposed legislation, but was instead added by the House Committee.[59] Although this division of punishment tracks the division for grand and petit larceny found in Virginia Code sections 18.2-95 and 18.2-96, the division is not in keeping with the approach of the entire Act which addresses intent, not the value or amount of damage caused.[60] The adopted division uses a reward system which benefits evil intentions that do not result in a tangible, definable damage. At a minimum, the term "value" should be defined so as to create some certainty in the degree of punishment. Suggested language would be:

> "Value" for purposes of this article shall be determined based on the greatest of the following:
>
> 1. the value of the property or services to the owner;
>
> 2. the value of the property or services to any other user of the computer or computer network;
>
> 3. the value of the property or services to the offender; or
>
> 4. the value of the property or servics to any third party affected by the alleged offense.

2. Computer Trespass

The crime of computer trespass[61] largely addresses those situations where the computer data or machinery is the object of the crime. Using a computer without authority with the intent to remove or alter any data, cause a computer malfunction, create an improper financial instrument, or cause any physical injury to any property are all considered computer trespass. The crime is punished as a Class 1 misdemeanor.

---

59. *Id.*

60. Indeed, an earlier version attempted to make such a distinction for all of the computer crimes related to damage to property. The distinctions were eliminated, however, since it was clear that an offender could easily attempt to cause extensive damage but ultimately not obtain the property or services sought.

61. VA. CODE ANN. § 18.2-152.4 (Cum. Supp. 1984).

Two caveats are necessary with regard to this crime. First, the value of the damage done is not relevant in considering punishment. Second, the Class 1 misdemeanor punishment is not unreasonably light since accomplishment of any of the objects of this crime will be punished as a separate crime. It is important to realize that the punishment is intended to deter efforts to access a computer, regardless of success.

3. Computer Invasion of Privacy

The next crime defined is computer invasion of privacy.[62] The activity proscribed under this label is the use of a computer, without authority, to examine personal information relating to any other person. This crime is punished as a Class 3 misdemeanor which carries a maximum fine of $500.[63] The examination of personal information is limited to those situations where the offender continues to view information which he knows or should know he is without authority to review.

The House Committee made two additions to the proposed language for this crime. First, the Committee added the requirement that not only must the *review of the information* be without authority,[64] but the *use of the computer* must also be without authority. The purpose of this addition is not clear and is arguably superfluous because the definition of without authority includes the use of a computer for a reason beyond the scope of authority.

The second Committee amendment required that the examination of the information must be "with the intent to injure such person."[65] An argument can be made that this addition is also without effect since the review of personal information regarding another person may always have some injurious effect, even if purely emotional. A difficult problem exists, however, with the nosey individual who has access to some data files and randomly looks at information regarding others. While the House Committee believed that the intent to injure will likely be inferred in cases deemed egregious enough to warrant prosecuting, it will take some experience with actual prosecutions under this section to understand the effect of this second addition.

---

62. *Id.* § 18.2-152.5 (Cum. Supp. 1984).
63. *Id.* § 18.2-11(c) (Repl. Vol. 1982).
64. *Id.* § 18.2-152.5 (Cum. Supp. 1984).
65. *Id.*

4. Theft of Computer Services

Theft of computer services[66] is a catch-all crime which includes any improper use of a computer which does not fit into any other category. This crime is punishable as a Class 1 misdemeanor.

5. Personal Trespass by Computer

The final new crime defined in the Act is the crime of personal trespass by computer.[67] This crime requires the use of a computer without authority and with the intent to cause physical injury to another. The 414's strike on the Sloan-Kettering computer which contained treatment data on cancer patients[68] or the interference with a computer controlling electric power, air traffic control, or vehicle traffic lights would be punished under this section. If committed maliciously, the crime is punished with the most serious penalty found in the Act: a Class 3 felony which carries a term of imprisonment of from five to twenty years.[69] All other acts of personal trespass by computer are punished as Class 1 misdemeanors. If actual personal injury is caused such as homicide or malicious wounding, separate and additional punishment would be available.

6. Embezzlement

Although a new crime is not defined, the Act recognizes that the deletion of Virginia Code section 18.2-98.1 leaves a gap in the crime of embezzlement because computer time and services would no longer be the subject of a prosecution for embezzlement. Accordingly, a section was included defining personal property subject to embezzlement under Virginia Code section 18.2-111 as all items included in the definition of property under the Act except for real property, which is not considered a proper object of embezzlement.[70]

---

66. *Id.* § 18.2-152.6 (Cum. Supp. 1984).

67. *Id.* § 18.2-152.7 (Cum. Supp. 1984).

68. *See supra* note 17 and accompanying text.

69. VA. CODE ANN. § 18.2-10(c) (Repl. Vol. 1982).

70. *Id.* § 18.2-152.8 (Cum. Supp. 1984).

D. *Procedural Provisions*

1. Statute of Limitations

Recognizing the difficulty of detecting many computer-related crimes, the legislature lengthened the usual statute of limitations for prosecution of computer crimes. The normal time limitation in which a prosecution for a misdemeanor must commence is one year.[71] The Act permits prosecution until the earlier of five years after the last act in the course of conduct occurred, or one year after the act and the identity of the offender is discovered by the state, the owner, or by anyone else damaged by the offense.[72] Thus, the one-year period is preserved, but only from the time the offender can be prosecuted. Otherwise, a five-year period is the maximum time in which a prosecution can be brought. This provision encourages a computer owner to detect the occurrence of illegal activity without giving the more talented offender who can disguise his actions too short a statute of limitations. Prosecutions for a felony can be brought at any time under a general provision in the Virginia Code.[73]

2. Venue

A current topic of debate where computer crime legislation is under consideration is the location in which a particular crime can be prosecuted. The Virginia Act defines the venue for prosecution as the location where any act was performed, where the owner has his principal place of business, where the offender held any of the proceeds from or materials used in the crime, where any communications took place to gain access to the computer or network, or where the offender resides.[74] Presumably, if the offender starts the act in another state but affects a computer in Virginia, the Commonwealth could have the criminal extradited back to Virginia.[75]

---

71. *Id.* § 19.2-8 (Repl. Vol. 1983).

72. *Id.* § 18.2-152.9 (Cum. Supp. 1984).

73. *Id.* § 19.2-243.

74. *Id.* § 18.2-152.10.

75. Uniformity of legislation among the states would encourage cooperation since all states would have an equal interest in insuring that the mechanisms for enforcement for the various states would be effective. While there may be constitutional limitations regarding the powers of the various states, cooperation between states can reduce the difficulties of extradition to only such constitutional limitations.

availability of this protection to state judges.[80]

The statute of limitations for civil remedies takes the same approach followed in the criminal provision.[81] Recognizing the difficulty of detection, the legislature provided that civil actions under the Act could be brought at any time up to the earlier of five years after the last act in the course of conduct or two years after the plaintiff discovered *or should have discovered* the last act in the course of conduct.[82] Thus, some responsibility is placed on the owner to determine when improper access occurs.

Three provisions, all contained in Virginia Code section 18.2-500, were removed from the proposed version of the Act prior to approval by the House. First, the provision allowing an injunction as a remedy was removed since the House believed that such a remedy would always be available in appropriate circumstances. Similarly, a provision allowing automatic treble damages for the successful plaintiff was deleted. Because punitive damages are already allowed in appropriate cases of malicious activity, the legislature believed that it was not necessary to restate an existing principal of law. The third provision removed by the House would have allowed the successful computer owner to collect attorney's fees. Virginia follows the common law approach toward counsel fees, and the courts routinely deny the award of fees unless there is contractual or statutory authority for such action,[83] or where exemplary damages are awarded for wanton or malicious behavior.[84] Prior attempts to include provisions for attorney's fees in legislation in Virginia have been generally unsuccessful.[85] Accordingly, to prevent the Act from becoming controversial on that basis alone, the provision for attorney's fees was removed.

---

80. VA. CODE ANN. § 18.2-152.12(B) (Cum. Supp. 1984).

81. *See supra* notes 71-73 and accompanying text.

82. VA. CODE ANN. § 18.2-152.12(D) (Cum. Supp. 1984).

83. *See* East Texas Salvage & Mach. v. Duncan, 226 Va. 160, 161, 306 S.E.2d 896, 897 (1983); Hiss v. Friedberg, 201 Va. 572, 577, 112 S.E.2d 871, 875 (1960).

84. Kemp v. Miller, 166 Va. 661, 680, 186 S.E. 99, 106 (1983).

85. An unusual exception to the trend in Virginia is found in VA. CODE ANN. § 18.2-500(a) (Repl. Vol. 1982) which provides for civil relief for combination to injure others in their reputation, trade, business or profession.

3. Effect on Other Crimes

The Act specifically directs that the crimes defined therein must be treated separately from all other crimes in the Virginia Code "unless . . . [such interpretation would be] clearly inconsistent with the terms of this article."[76] This provision was included for two reasons. First, the provision emphasizes that the Act defines new crimes instead of modifying existing ones. In short, a new set of tools are provided to judges, prosecutors and defense lawyers instead of forcing old pegs into new holes. Second, in many instances where significant property damage and personal injury occurs, additional punishment would be justified.

E. *Civil Relief*

The section of the Act which provides for civil relief to the injured party[77] has received a great deal of attention throughout the country. In effect, the provision allows the computer owner to recover for any losses incurred due to the criminal activity. The structure for this provision came from another section in the Virginia Criminal Code which provides for civil relief, including an injunction and treble damages, where the offender has interfered with the business of another.[78]

However, bringing a civil action may sometimes have negative consequences. During a prosecution for unauthorized use of a computer system, evidence is often presented which describes the method by which the system security was broken. Publicizing this information may facilitate the current prosecution, but the owner may be forced to ensure that an onlooker does not try to repeat the crime. The owner must also make sure that valuable trade secrets are not disclosed. Case law developing throughout the country has confirmed that trade secrets in civil actions may be treated by courts in such a way as to protect their secrecy while accomplishing the purpose of the litigation.[79] An additional paragraph was inserted in the Virginia Computer Crimes Act to emphasize the

76. VA. CODE ANN. § 18.2-152.11 (Cum. Supp. 1984).

77. *Id.* § 18.2-152.12.

78. *Id.* § 18.2-500 (Repl. Vol. 1982).

79. *See, e.g.*, Reliance Ins. Co. v. Barron's, 428 F. Supp. 200 (S.D.N.Y. 1977); Davis v. General Motors Corp., 64 F.R.D. 420 (N.D. Ill. 1974); Marshwood Co. v. Jamie Mills, Inc., 10 F.R.D. 386 (N.D. Ohio 1950).

F. *Miscellaneous Provisions*

1. Severability

A severability provision[86] was included in the legislation so that if any portion of the Act was found to be invalid, the legislature's expectations would be carried out to the fullest extent possible. This provision was considered particularly important since the Act can have far-reaching criminal and civil implications and may be affected by federal legislation or court decisions.

2. Forgery

The final provision in the statute directs that a forgery can be prosecuted if computer data is created, altered, or deleted even if no physical "writing" occurs.[87] The Act does require that the activity, if done on a tangible document, would have to constitute a forgery.

G. *Conduct of Criminal Proceedings*

The House Committee deleted a proposal which would have permitted a court to conduct any criminal proceedings in private if the proceedings required the owner to reveal his trade secrets or facilitated repetition of the proscribed activity. This omission may diminish the ability of the state to obtain cooperative witnesses, because such witnesses may have to choose between punishing the offender and preventing a proliferation of the infiltration.

The major justification for the House Committee's deletion was a concern for the criminal's right to a public trial guaranteed in both the sixth amendment of the United States Constitution and in article I, section 8 of the Virginia Constitution. If this issue is discussed before the same House Committee again, it should be noted that the right to a public trial is not an absolute right, but rather, is a right which can be curbed where sensitive data is to be released.[88] Additional protective language could be added to the

86. VA. CODE ANN. § 18.2-152.13 (Cum. Supp. 1984).

87. *Id.* § 18.2-152.14.

88. *See, e.g.*, Globe Newspaper Co. v. Superior Court, 102 S. Ct. 2613 (1982) (closure of trial permitted in certain circumstances); United States v. Ruiz-Estella, 481 F.2d 723 (2d Cir. 1973) (non-public proceedings were allowed in order to protect the contents of a "confidential hijacking profile"); Perez v. Metz, 459 F. Supp. 1131 (S.D.N.Y. 1977) (witnesses were in fear of their lives).

section as originally proposed so that the provision would read as follows:

> *Conduct of Proceedings.* — At the request of the owner of the computer, computer network, computer data, computer program, or computer software which was involved in any act in violation of this article, the court may, in its discretion and upon good cause shown, conduct all legal proceedings under this article in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets involved. The court's discretion under this section shall be exercised in such a way as to balance (a) the offender's important right to a public trial with (b) the Commonwealth's compelling public interests in avoiding the recurrence of the same or similar acts, in encouraging the prosecution of the crimes defined under this article, in encouraging complete and truthful testimony so that the offender is fully tried with all facts brought to the attention of the trier of fact, and in protecting the trade secrets of the owner, if any of such compelling interests are in fact present in the instant case. The court shall conduct only so much of the proceedings in secret as shall be absolutely necessary to promote these compelling public interests of the Commonwealth. Before any proceedings are held in secrecy, the court shall enter an order detailing those facts which it had taken into consideration when ordering the secret proceeding and specifying the precise matters which will be tried in secret.

IV. Critics' Reviews

By enacting the Virginia Computer Crimes Act, the Virginia General Assembly addressed a large number of issues confronting today's computer and computer network owners. The legislation needs some technical modifications, and more consideration should be given to protecting the secrecy of the "invaded" computers and the proprietary information of the owners.

In the meantime, many non-legislative solutions will continue to be posed to deter or capture the would-be offender. Perhaps the ultimate deterrent will be based on a combination of improved security mechanisms and the fear of legislation such as the Virginia Computer Crimes Act. Until then . . .

HOW ABOUT A GOOD GAME OF CHESS, JESSIE JAMES?

ADDENDUM

The 1985 General Assembly was again given the opportunity to address several of the provisions discussed in the body of the preceding article, but due largely to the shortened session of the General Assembly and to several other very controversial bills, the legislature's efforts solved few of the issues raised by the amendments.

One amendment, signed into law by the Governor on March 5, 1985, simply relocated the specific terms of the statute of limitations for a civil action related to injury from a violation of the Computer Crimes Act to Section 8.01-40.1 because Title 8.01 contains all of the various civil statutes of limitations.[1]

A second amendment approved by both houses of the General Assembly[2] made the technical correction to the Act to include "or computer network" in each newly-defined crime.[3] The same bill also included an additional subpart to the definition of "computer trespass".[4] As a result, making any unauthorized copies "of computer data, computer programs or computer software residing in, communicated by or produced by a computer or computer network" will become a form of computer trespass. It should be noted that the subpart may be preempted by the Federal Copyright Act.[5] A third addition as a result of this particular amendment allows venue for criminal prosecution where a computer which is the object or instrument of the violation is located.

The third bill approved by the General Assembly[6] returned the language of Section 18.2-152.5 ("Computer invasion of privacy") to its form prior to the amendments introducd by the House Courts

---

1. 1985 Va. Act ch. 92.

2. Va. H. 1470, 1985 Va. Acts ___. As of this writing, this Bill had not been signed by the Governor, but it is expected that he will sign it imminently.

3. This change corrected the drafting error discussed *supra* note 41 and accompanying text.

4. VA. CODE ANN. § 18.2-152.4 (Cum. Supp. 1984).

5. 17 U.S.C. §§ 101-810 (1982). The issue of whether the Copyright Act preempts this provision is beyond the scope of this Addendum. If a court does conclude that Congress intended to preempt this type of provision, the severability provision contained in VA. CODE ANN. § 18.2-152.13 (Cum. Supp. 1984) should limit the effect of the preemption to this new subpart.

6. Va. H. 1468, 1985 Va. Acts ___. This bill had not been signed by the Governor as of this writing.

of Justice Committee in 1984.[7] In addition, the phrase "or computer network" was also added to the definition of this crime.

Several amendments were, on the other hand, rejected by the General Assembly. Provisions defining "value" and requiring the aggregation of losses to determine the classification of crimes were not accepted.[8] Furthermore, a provision setting forth a basis for long arm statute coverage of an out-of-state actor causing civil damage within the state was deleted.[9] The reason given by the House Courts of Justice Committee was that the present long arm statute[10] has sufficient coverage. The "conduct of proceedings" concept discussion in the main article[11] was again rejected in 1985.[12] Finally, language to "undo" the House's 1984 revisions to the definition of "without authority"[13] was rejected.[14]

7. *See supra* notes 62-65.
8. Va. H. 1465, 1985 Va. Acts ___. *See supra* notes 58-60.
9. Va. H. 1466, 1985 Va. Acts ___.
10. VA. CODE ANN. §§ 8.01-328 to -330 (Repl. Vol. 1984).
11. *See supra* note 88.
12. Va. H. 1467, 1985 Va. Acts ___.
13. VA. CODE ANN. § 18.2-152.2 (Cum. Supp. 1984). *See supra* notes 55-57.
14. Va. H. 1469, 1985 Va. Acts ___.