

# William & Mary Law Review

---

Volume 27 (1985-1986)

Issue 4 *The Seventh Anglo-American Exchange:  
Judicial Review of Administrative and  
Regulatory Action*

---

Article 11

May 1986

## Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act

Robin K. Kutz

Follow this and additional works at: <https://scholarship.law.wm.edu/wmlr>



Part of the [Science and Technology Law Commons](#)

---

### Repository Citation

Robin K. Kutz, *Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act*, 27 Wm. & Mary L. Rev. 783 (1986),  
<https://scholarship.law.wm.edu/wmlr/vol27/iss4/11>

Copyright c 1986 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.

<https://scholarship.law.wm.edu/wmlr>

## NOTES

### COMPUTER CRIME IN VIRGINIA: A CRITICAL EXAMINATION OF THE CRIMINAL OFFENSES IN THE VIRGINIA COMPUTER CRIMES ACT

Thanks to the computer, "[t]he 'information revolution' that futurists have long predicted has arrived, bringing with it the promise of dramatic changes in the way people live and work, perhaps even in the way they think. America will never be the same."<sup>1</sup>

This quotation aptly describes the position that the computer has assumed in modern society. Large "mainframe" computers predict the weather, process checks, scrutinize tax returns, guide intercontinental missiles,<sup>2</sup> launch and land the space shuttle, model the predicted behavior of a nuclear reactor in an emergency,<sup>3</sup> and perform a multitude of important tasks for governmental,<sup>4</sup> educational,<sup>5</sup> and commercial<sup>6</sup> institutions. The "personal

---

1. Friedrich, *The Computer Moves In*, TIME, Jan. 3, 1983, at 14 (Special Section: "Machine of the Year"). Friedrich declared: "Time's Man of the Year for 1982, the greatest influence for good or evil, is not a man at all. It is a machine: the computer." *Id.* at 16.

2. *Id.* at 14.

3. Baldwin, *Faster, Faster, Faster*, FORBES, Oct. 24, 1983, at 189.

4. Computer use in government has grown rapidly. In 1979, the federal government operated nearly 12,000 computers. 125 CONG. REC. 1195 (1979) (statement of Donald L. Scanlebury, Dir. of Fin. & Gen. Mgmt. Studies Div., GAO). By 1983, that number exceeded 15,000, with the Bureau of Census and the Department of Defense using most of the computers. 129 CONG. REC. S11,448 (daily ed. Aug. 3, 1983) (statement of Sen. Tribble). In early 1984, the reported figures were "18,000 medium and large-scale computers at some 4,500 sites," and the General Services Administration estimated that the federal government "could have between 250,000 and 500,000 [microcomputers] in place by 1990." 130 CONG. REC. S1180 (daily ed. Feb. 8, 1984) (statement of Sen. Cohen).

5. One commentator reported that "American schools possess more than 100,000 computers for school use and student training." Note, *Computer Abuse: The Emerging Crime and the Need for Legislation*, 12 FORDHAM URB. L.J. 73, 73 n.8 (1984).

6. According to a recent Note, "businesses rely on more than 56,000 large general purpose computers, 213,000 smaller business computers, 570,000 minicomputers, and 2.4 million desktop computers, with over three million computer terminals in business offices." *Id.* at 74 n.10.

computer"<sup>7</sup> has revolutionized small business, permitting even one-man operations to compete in the marketplace.<sup>8</sup> The computer "network"<sup>9</sup> has brought the world to the home, and the microprocessor<sup>10</sup> has vastly improved many consumer products.<sup>11</sup> In short, the computer is ubiquitous.

Unfortunately, the computer revolution also has sired a new category of criminal activity: computer-assisted crime.<sup>12</sup> Some of these

7. "Personal computer" is the common name for a microcomputer, which is defined as "a small computer (in terms of data storage) whose central processing unit is contained on either a small circuit board or within a single integrated circuit chip." F. RHOADS & J. EDWARDS, *LAW OFFICE GUIDE TO SMALL COMPUTERS* § 1.05, at 7 (1984).

8. See Friedrich, *supra* note 1, at 17-18.

9. A "network" is composed of two or more remotely located computers connected by a communications link. See *infra* note 27. The owner of a computer equipped with a telecommunication link can use any of approximately 1450 electronic user data services ranging from "the Source, a *Reader's Digest* subsidiary in McLean, Va., which can provide stock prices, airline schedules or movie reviews, to more specialized services like the American Medical Association's AMA/NET, to real esoterica like the Hughes Rotary Rig Report." Friedrich, *supra* note 1, at 17. Computer owners with similar machines or interests also form "bulletin boards" to swap information and computer programs of interest to members or to the general public. See Plantz, *BBS Watch*, *PC WORLD*, May 1983, at 328.

10. A microprocessor, which is a miniature central processing unit (CPU), consists of the integrated circuitry that directs the flow of information within the computer and does the actual computing. A *Guide to Compuspeak*, *CONSUMER REPS.*, Sept. 1983, at 486-87. The microprocessor thus is the actual "computer." The remainder of the computer system's physical parts ("hardware") combine with the computer programs and data files ("software") to define the full capabilities of a computer system.

11. A microprocessor containing customized operating instructions "written" permanently in its integrated circuitry, a feature known as "read-only memory" (ROM), can be installed inside a machine to control or monitor its operation. This technological advance has permitted, among other things, the increased sophistication of many household appliances, such as microwave ovens, televisions, and digital clocks. Kindel & Teitleman, *But What Do I Use It For?*, *FORBES*, Oct. 24, 1983, at 76, 80. One recent advertisement even touted a table saw fitted with a microprocessor: "Just push a button on the front-mounted computerized panel to raise or lower the blade an incredibly accurate .005 inch. . . . Programmable for bevel, elevation and shutdowns." SEARS, ROEBUCK & Co., 1985 SPRING/SUMMER CATALOG 696 (1984).

12. Most commentators refer to this category of criminal activity as "computer crime." See, e.g., S. MANDELL, *COMPUTERS, DATA PROCESSING, AND THE LAW* 154-71 (1984); Roddy, *The Federal Computer Systems Protection Act*, 7 *RUTGERS J. COMP. TECH. L.* 343, 344-45 (1980); Note, *A Suggested Legislative Approach to the Problem of Computer Crime*, 38 *WASH. & LEE L. REV.* 1173, 1175 (1981).

One commentator has suggested "computer-assisted crime" as a more appropriate phrase because the only crimes "which present special challenges to those involved in the prevention, detection, investigation, and prosecution of white-collar crime" are those involving actual use of a computer. J. BECKER, *THE INVESTIGATION OF COMPUTER CRIME* 1 (1980). This Note adopts Becker's "computer-assisted crime" designation because it focuses solely on crimes that involve computer use. Legislation aimed at computer-assisted criminal activity

crimes have involved fantastic sums. For example, the Equity Funding insurance scam reportedly involved \$2 billion,<sup>13</sup> the Security Pacific National Bank theft involved \$10.2 million,<sup>14</sup> and the Union Dime Savings Bank embezzlement netted \$1.4 million.<sup>15</sup> These cases have fascinated the press, have intrigued the public, and have worried law enforcement officials and legislators alike. Equally disturbing has been the 1973 Stanford Research Institute (SRI) study,<sup>16</sup> which estimated that the annual worldwide loss from computer abuse was \$300 million, and that the average take was \$450,000.<sup>17</sup> The SRI study revealed not only a generally higher per incident loss rate for computer-assisted crimes than for other white collar crimes, but also that the losses for each type of computer-assisted crime might be greater than those for the equivalent crime accomplished without a computer.<sup>18</sup> During the 1970's, law

---

should ignore acts in which the computer is only the *object* of the crime, such as sabotage or other physical assaults. These crimes are covered adequately by vandalism, malicious mischief, and sabotage statutes, and do not pose problems for prosecutors. Gemignani, *Computer Crime: The Law in '80*, 13 IND. L. REV. 681, 682 (1980); Taber, *On Computer Crime* (Senate Bill S. 240), 1 COMP. L.J. 517, 525 (1979). See generally T. WHITESIDE, *COMPUTER CAPERS* 4-7 (1978) (examples of physical attacks on computers).

13. S. MANDELL, *supra* note 12, at 161-62; see also T. WHITESIDE, *supra* note 12, at 11-18 (describing the crime in detail). The \$2 billion figure includes the estimated market losses suffered by the Equity Funding Corporation stockholders; the audited figures estimated only a \$200 million loss. D. PARKER, *CRIME BY COMPUTER* 28 (1976).

14. Becker, *Rifkin, A Documentary History*, 2 COMP. L.J. 471, 474 (1980).

15. D. PARKER, *supra* note 13, at 192-203.

16. D. PARKER, S. NYCUM & S. OURA, *COMPUTER ABUSE* (1973).

17. See D. PARKER, *supra* note 13, at 28-30. The SRI figures have stirred some controversy. After exhaustive analysis, one commentator concluded that the SRI study is "unreliable because it is based on poor documentation, unacceptable methods, and unverified (indeed unverifiable) losses." Taber, *A Survey of Computer Crime Studies*, 2 COMP. L.J. 275, 310 (1980). This same commentator analyzed a GAO study that concluded that the average computer crime loss was \$44,110—less than one-tenth of the SRI estimate. He concluded that the GAO figures were more reliable than the SRI figures. *Id.* at 282-83 & n.44. Although Donn Parker, a member of the SRI panel, admitted that he did not know the statistical validity of the SRI's figures, D. PARKER, *supra* note 13, at 28, the tenor of his statistical discussion indicates that he believed the estimates to be basically sound. See *id.* at 23-30.

At least one commentator has concluded that the discrepancies between the findings of the two studies reveal fundamental research problems and not simply data collecting biases. See S. MANDELL, *supra* note 12, at 156. Regardless of the statistical validity issue, however, legislatures have enacted computer-assisted crime legislation at least partially in response to alarmist reports such as the SRI study. The question no longer is whether this country has a computer-assisted crime problem that needs legislative attention; it is whether the recently enacted legislation will permit successful prosecution of computer-assisted crimes.

18. D. PARKER, *supra* note 13, at 32-33. According to Mr. Parker:

enforcement authorities also began to realize that many computer-assisted crimes were easy to accomplish but difficult to detect.<sup>19</sup> They discovered that most computer-assisted crimes either went

---

Assets tend to be more highly concentrated in computer systems than in equivalent manual systems. [Once access to the funds is accomplished] it is just as easy [for the computer-assisted perpetrator] to steal a million dollars as it is one dollar. . . . [Further,] the opportunity for theft of larger amounts . . . is far greater with the same or smaller amount of effort by the perpetrator.

*Id.* at 33; accord Taber, *supra* note 17, at 287 & n.49.

A comparison of traditional and computer-assisted bank robbers illustrates Parker's thesis. Traditional robbers, who physically enter banks to carry out their crimes, are limited not only by the amount of cash in the tellers' drawers or in the vault, but also by the amount of money they can carry. On the other hand, once computer-assisted bank robbers "enter" banks via computer, they quickly can transfer enormous sums to another bank account simply by pressing the right buttons, and the sums available to computer-assisted robbers typically far exceed the cash stored in the banks themselves. *Cf.* Becker, *supra* note 14 (explaining how the Security Pacific National Bank theft was accomplished).

19. Fraudulent data crimes and theft of computer services are perhaps the easiest computer-assisted crimes to commit and the most difficult to detect, which probably explains why they are so prevalent.

GAO studies have shown that "the majority of computer crimes against the Federal government—about 62%—involved [fraudulent data input]." 125 CONG. REC. 1195 (1979) (statement of Donald L. Scantlebury, Dir. of Fin. & Gen. Mgmt. Studies Div., GAO); *see also* Roddy, *supra* note 12, at 348 n.40 (placing the figure at 62-80%). Either an operator who types information into a computer or an unauthorized user who alters existing data can accomplish fraudulent data entry. Detection is difficult for two reasons. First, "literally millions of Federal actions take place regularly on automated systems without anyone checking them for correctness." *Id.* Second, even if someone does attempt to run a check, stored computer data is invisible until actually printed. The printout obtained after a fraudulent data entry has occurred will appear perfectly normal, and the altered data will appear suspicious only if the figures are abnormally high or low. *See, e.g.,* 130 CONG. REC. S1179 (daily ed. Feb. 8, 1984) (remarks of Sen. Cohen) (noting that hackers had penetrated credit bureau computer and had changed credit ratings of prominent persons); 130 CONG. REC. E633 (daily ed. Feb. 27, 1984) (remarks of Rep. Wyden) (noting that hackers had gained access to cancer patient records at Sloane Kettering Cancer Center and had gained ability to change radiation doses).

The other prevalent computer crime, theft of computer services, apparently is a widespread problem in the business world. Some businesses even condone the problem. Taber, *supra* note 12, at 530-31; *see infra* note 20; *infra* note 223 and accompanying text. Thefts of computer services often are discovered only by accident. *See, e.g.,* *United States v. Seidlitz*, 589 F.2d 152, 154 & n.5 (4th Cir. 1978) (computer specialist noticed an access code in use that belonged to a supervisor not then using the computer), *cert. denied*, 441 U.S. 922 (1979); Gemignani, *supra* note 12, at 713-18 (discussing *State v. Thommen*, No. 79-424B (Ind. Crim. Ct. Feb. 14, 1980) (fellow employee noticed computer printout of highly confidential program on defendant's desk)); *cf.* *State v. McGraw*, 459 N.E.2d 61, 63 (Ind. Ct. App. 1984) (defendant's unauthorized use was revealed, after his dismissal, when former colleague refused to copy defendant's illegal data files); *Lund v. Commonwealth*, 217 Va. 688, 689-90, 232 S.E.2d 745, 747 (1977) (graduate student who charged computer time worth

undiscovered or unreported<sup>20</sup> and, perhaps most importantly, that existing laws could not handle the novel aspects of computer-assisted crime.<sup>21</sup>

These considerations led the Senate Governmental Affairs Committee in 1976 to examine the need for federal computer crime legislation.<sup>22</sup> One year later, Senator Abraham Ribicoff introduced S. 1766, the first Federal Computer Systems Protection Act.<sup>23</sup> Although this bill never passed Congress, each succeeding Congress has considered comprehensive federal computer-assisted crime legislation.<sup>24</sup> Pressure to enact this type of legislation was particularly

---

more than \$26,000 to various university departments was caught when the departments finally complained about the unauthorized charges).

20. Many victimized businesses prefer for several reasons not to report computer-assisted crimes. Some businesses, especially financial institutions, seem to fear lessened public confidence, which may result in declining stock value, lower employee morale, and lost business. 129 CONG. REC. E2429 (daily ed. May 19, 1983) (statement of Rep. Wyden); J. BECKER, *supra* note 12, at 5; Roddy, *supra* note 12, at 347 n.34; Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMP. L.J. 353, 359 (1980). Others fear that trial publicity may prompt a subsequent break-in, and that they will not be able to secure the computer. Sokolik, *supra*, at 359. Other concerns include a belief that the benefits gained from a conviction do not outweigh the costs of assisting in the investigation and prosecution of the case, J. BECKER, *supra* note 12, at 6, and skepticism about the effectiveness of the criminal justice system, *id.*

21. The existing laws are deficient primarily in defining the common law crime of larceny, R. PERKINS & R. BOYCE, CRIMINAL LAW 292 (3d ed. 1982), and its statutory relatives—embezzlement, *id.* at 354, and false pretenses, *id.* at 364. Difficulties that may arise in computer-assisted crime cases involving these crimes include: (1) the possibility that the court may find that computer-related intangibles are not “property” for the purposes of a larceny prosecution, *see Ward v. Superior Court*, 3 CLSR 206 (Cal. Super. Ct. 1972) (electronic impulses); *Lund v. Commonwealth*, 217 Va. 688, 692, 232 S.E.2d 745, 748 (1977) (computer time and services); (2) the possibility that the jury may not find that the defendant intended permanently to deprive the true owner of possession, *see S. MANDELL, supra* note 12, at 164; and (3) the lack of any easy method to calculate the market value of computer-related intangibles, such as computer data or programs, which may prompt courts to use the actual value of the tangible property involved as the value of the goods stolen, *see e.g., Lund v. Commonwealth*, 217 Va. 688, 692, 232 S.E.2d 745, 748 (1977) (holding that, in the absence of market value, the court must use the actual value of a computer printout—the scrap value of the paper).

22. 125 CONG. REC. 1191 (1979) (statement of Sen. Ribicoff).

23. S. 1766, 95th Cong., 1st Sess., 123 CONG. REC. 21,025 (1977); *see also Federal Computer Systems Protection Act: Hearings on S. 1766 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary*, 95th Cong., 2d Sess. 1 (1978) [hereinafter cited as *Hearings, S. 1766*]. An identical bill was introduced in the House of Representatives. H.R. 8421, 95th Cong., 1st Sess., 123 CONG. REC. 23,720 (1977).

24. H.R. 930, 99th Cong., 2d Sess., 131 CONG. REC. H294 (daily ed. Feb. 4, 1985); S. 2940, 98th Cong., 2d Sess., 130 CONG. REC. S10,257 (daily ed. Aug. 9, 1984); S. 2270, 98th Cong., 2d

strong in 1983 and 1984, when twelve related bills also were introduced in Congress.<sup>25</sup> This legislative surge may have been prompted by the increasing popularity and availability of inexpensive personal computers<sup>26</sup> and of the communications devices required to link them.<sup>27</sup> These technological advances have

---

Sess., 130 CONG. REC. S1180 (daily ed. Feb. 8, 1984); S. 1733, 98th Cong., 1st Sess., 129 CONG. REC. S11,448 (daily ed. Aug. 3, 1983); H.R. 1092, 98th Cong., 1st Sess., 129 CONG. REC. H219 (daily ed. Jan. 31, 1983) (companion bill to S. 1733); H.R. 3970, 97th Cong., 1st Sess., 127 CONG. REC. 13,014 (1981); H.R. 6192, 96th Cong., 1st Sess., 125 CONG. REC. 36,991 (1979); S. 240, 96th Cong., 1st Sess., 125 CONG. REC. 1190 (1979) (companion bill to H.R. 6192).

25. These proposals addressed many aspects of computer-assisted crime, including abuse of the social security system equipment and resources, H.R. 2619, 98th Cong., 1st Sess., 129 CONG. REC. H2190 (daily ed. Apr. 19, 1983), protection from computer-assisted crime for small businesses, S. 1920, 98th Cong., 1st Sess., 129 CONG. REC. S13,560 (daily ed. Oct. 4, 1983); H.R. 3075, 98th Cong., 1st Sess., 129 CONG. REC. H3144, E2429 (daily ed. May 19, 1983) (companion bill to S. 1920) (enacted July 16, 1984), counterfeiting of access devices, and computer fraud and abuse, H.R. 3570, 98th Cong., 1st Sess., 129 CONG. REC. H5196 (daily ed. July 14, 1983), criminal penalties for computer abuse, H.R. 4259, 98th Cong., 1st Sess., 129 CONG. REC. H8907 (daily ed. Oct. 31, 1983) (also proposing an interagency committee to consider computer crime and abuse), other computer-assisted crimes, H.R. 4301, 98th Cong., 1st Sess., 129 CONG. REC. H9212 (daily ed. Nov. 3, 1983), unauthorized access to medical records via telecommunication devices, H.R. 4954, 98th Cong., 2d Sess., 130 CONG. REC. H916 (daily ed. Feb. 27, 1984), counterfeiting of access devices and other computer fraud and abuse, H.R. 5112, 98th Cong., 2d Sess., 130 CONG. REC. H1574 (daily ed. Mar. 13, 1984) (evolved from H.R. 3570), fraud and related activities connected with access devices and computers, S. 2862, 98th Cong., 2d Sess., 130 CONG. REC. S9223 (daily ed. July 25, 1984); H.R. 5616, 98th Cong., 2d Sess., 130 CONG. REC. H3561 (daily ed. May 8, 1984) (companion bill to S. 2862) (enacted Oct. 12, 1984), unauthorized direct access to or alteration of individual medical records via telecommunication devices, H.R. 5831, 98th Cong., 2d Sess., 130 CONG. REC. H5677 (daily ed. June 12, 1984) (passed House, 130 CONG. REC. H9637 (daily ed. Sept. 17, 1984)), and computer fraud involving interstate or foreign commerce, S. 2940, 98th Cong., 2d Sess., 130 CONG. REC. S10,257 (daily ed. Aug. 9, 1984).

Two of these twelve bills became law in 1984. H.R. 3075 was enacted as the Small Business Computer Security and Education Act of 1984, Pub. L. No. 98-362, 98 Stat. 431 (codified at 15 U.S.C.A. §§ 632(j)(1)(A)-(B), 633(b)(3), 637(b)(1)(A) (West Supp. 1986)), and H.R. 5616 was enacted as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (codified at 18 U.S.C.A. § 1030 (West Supp. 1986)).

26. In 1981, all computer manufacturers together sold 500,000 computers suitable for home use. Just two years later, in September 1983, one computer magazine publisher predicted that IBM alone would sell 2,000,000 personal computers in 1984. Bunnell, *PC 1984*, *PC WORLD*, Jan. 1984, at 14. One survey of 20 personal computer manufacturers indicated a price range of \$799 to \$12,995. See F. RHOADS & J. EDWARDS, *supra* note 7, §§ 2.07-2.27.

27. Remotely located computers communicate primarily through "modems" (modulator-demodulators), which convert digital output signals containing computer data to analog signals that can be transferred over telephone lines. Jordan, *The Modem Market*, *PC WORLD*, Nov. 1983, at 88. The market for modems has been described as "exploding," *id.*, and one

spawned numerous instances of vandalism and mischief by "hackers," many of whom are adolescents.<sup>28</sup> With hackers' exploits attracting widespread media attention, congressional concern mounted, resulting in the numerous computer-related bills introduced in Congress in 1983 and 1984.<sup>29</sup>

State legislatures have acted against computer-assisted crime far more swiftly and more successfully than Congress. Beginning with Arizona, which acted in 1978,<sup>30</sup> forty-five states have enacted computer-assisted crime legislation. Twenty-three<sup>31</sup> of these states apparently modeled their statutes primarily on the 1977 or 1979 versions of the proposed Federal Computer Systems Protection Act,<sup>32</sup> while twenty<sup>33</sup> enacted comprehensive computer-assisted crime

survey of modem manufacturers indicated a price range of \$145 to \$1195, *see* Hayes, *Modems*, in *PC WORLD (ANNUAL HARDWARE REVIEW)* 134-43 (1984).

28. "Hackers" are individuals who use remotely located computers to break the security codes of other computer systems, thereby gaining unauthorized access to those systems through telephone linkups. For descriptions of several incidents involving hackers, *see Cracking Down on Hackers*, *NEWSWEEK*, Oct. 24, 1983, at 34; *Beware: Hackers at Play*, *NEWSWEEK*, Sept. 5, 1983, at 42-48; Dobbin, *Watch Out Roscoe, Susan Thunder, et al: Computer Criminals Get Caught*, *Baltimore Sun*, June 6, 1983, at —, col. — (reprinted in 129 *CONG. REC.* E2708 (daily ed. June 6, 1983)).

29. *See supra* note 25 and accompanying text.

30. *ARIZ. REV. STAT. ANN.* §§ 13-2301E, 13-2316 (1978 & Supp. 1986).

31. *ARIZ. REV. STAT. ANN.* §§ 13-2301E, 13-2316 (1978 & Supp. 1986); *CAL. PENAL CODE* § 502 (West Supp. 1986); *COLO. REV. STAT.* §§ 18-5.5-101 to -102 (1986); *DEL. CODE ANN.* tit. 11, §§ 931-939, 2738 (Supp. 1984); *GA. CODE ANN.* §§ 16-9-90 to -95 (1984); *HAWAII REV. STAT.* §§ 708-890 to -896 (Supp. 1984); *IDAHO CODE* §§ 18-2201 to -2202 (Supp. 1986); *KY. REV. STAT. ANN.* §§ 434.840 to .860 (1985); *MICH. COMP. LAWS ANN.* §§ 752.791 to .797 (West Supp. 1986); *MINN. STAT. ANN.* §§ 609.87 to .89 (West Supp. 1986); *MONT. CODE ANN.* §§ 45-2-101, 45-6-310 to -311 (1985); *NEV. REV. STAT.* §§ 205.473 to .477 (1986); *N.M. STAT. ANN.* §§ 30-16A-1 to -4 (1984); *N.C. GEN. STAT.* §§ 14-453 to -457 (1981); *N.D. CENT. CODE* §§ 12.1-06.1-01(3), 12.1-06.1-08 (1985); *OKLA. STAT. ANN.* tit. 21, §§ 1951-1956 (West Supp. 1985); *OR. REV. STAT.* § 164.377 (1985); 18 *PA. CONS. STAT. ANN.* § 3933 (Purdon Supp. 1986); *R.I. GEN. LAWS* §§ 11-52-1 to -5 (1981 & Supp. 1986); *S.C. CODE ANN.* §§ 16-16-10 to -40 (Law. Co-op. 1985); *TENN. CODE ANN.* §§ 39-3-1401 to -1406 (Supp. 1986); *UTAH CODE ANN.* §§ 76-6-701 to -704 (Supp. 1986); *WIS. STAT. ANN.* § 943.70 (West Supp. 1986).

32. S. 240, 96th Cong., 1st Sess., 125 *CONG. REC.* 1190 (1979); S. 1766, 95th Cong., 1st Sess., 123 *CONG. REC.* 21,025 (1977).

33. *ALA. CODE* §§ 13A-8-100 to -103 (Supp. 1986); *ALASKA STAT.* §§ 11.46.200(a)(3), .740, .985, .990(1), (3)-(7) (Supp. 1986); *CONN. GEN. STAT. ANN.* §§ 53a-250 to -261 (1985); *FLA. STAT. ANN.* §§ 815.02 to .07 (West Supp. 1986); *ILL. ANN. STAT.* ch. 38, ¶ 16-9 (Smith-Hurd Supp. 1986); *IND. CODE ANN.* §§ 35-43-1-4, -2-3 (Burns Supp. 1986); *IOWA CODE ANN.* §§ 716A.1 to .16 (West Supp. 1986); *KAN. STAT. ANN.* § 21-3755 (Supp. 1985); *LA. REV. STAT. ANN.* §§ 14:73.1 to .5 (West 1986); *MD. ANN. CODE* art. 27, § 146 (Supp. 1986); *MISS. CODE ANN.* §§ 97-45-1 to -13 (Supp. 1986); *MO. ANN. STAT.* §§ 569.093 to .099 (Vernon Supp.



statutes less closely related to the proposed federal legislation. The other two states, Ohio and Massachusetts, took another tack, choosing only to redefine certain terms in their criminal codes to ensure that their statutes covered computers and computer-related intangible property.<sup>34</sup> Ohio took the more expansive approach, by expanding its definitions of "property,"<sup>35</sup> "services,"<sup>36</sup> and "writing,"<sup>37</sup> and by adding six new computer-related definitions,<sup>38</sup> while Massachusetts chose only to redefine the term "property" in its larceny statute to include computer-related intangibles.<sup>39</sup>

The Virginia General Assembly originally responded to the computer-assisted crime problem by redefining the term "property" in its larceny statute in a manner similar to the Massachusetts statute.<sup>40</sup> The General Assembly repealed this statute in 1984,<sup>41</sup> however, and replaced it with the Virginia Computer Crimes Act<sup>42</sup> (Act). This comprehensive statute attempts to define and prohibit several categories of computer-assisted crime.

This Note scrutinizes the Virginia Computer Crimes Act to determine whether it has removed every obstacle to successful prosecution of those who commit computer-assisted crimes. The analysis begins with the computer-related definitions contained in the Act's glossary, and proceeds through each of the Act's penal sections, referring both to the proposed federal legislation and to the computer-assisted crime statutes of other states, when appropriate. The analysis reveals that, although the Act has solved some of the

---

1986); NEB. REV. STAT. §§ 28-1343 to -1348 (Supp. 1985); N.H. REV. STAT. ANN. §§ 638:16 to :19 (Supp. 1985); N.J. STAT. ANN. §§ 2C:20-1(g), :20-23 to -34 (West Supp. 1986); S.D. CODIFIED LAWS ANN. §§ 43-2-2, 43-43B-1 to -8 (1983 & Supp. 1984); TEX. PENAL CODE §§ 33.01 to .05 (Vernon Supp. 1986); VA. CODE §§ 18.2-152.1 to .14 (Supp. 1986); WASH. REV. CODE ANN. §§ 9A.48.100, .52.110 to .130, .56.010 (West 1977 & Supp. 1986); WYO. STAT. §§ 6-3-501 to -505 (1983 & Supp. 1986).

34. Alabama also took this approach at first, *see* ALA. CODE § 13A-8-10 (1982), but it subsequently enacted comprehensive computer-assisted crime legislation. *See id.* §§ 13A-8-100 to -103 (Supp. 1986).

35. OHIO REV. CODE ANN. § 2901.01(J) (Page Supp. 1985).

36. *Id.* § 2913.01(E).

37. *Id.* § 2913.01(F).

38. *Id.* § 2913.01(L)-(Q).

39. MASS. GEN. LAWS ANN. ch. 266, § 30(2) (West Supp. 1986).

40. VA. CODE § 18.2-98.1 (1982) (repealed 1984).

41. Act of Apr. 11, 1984, ch. 751, 1984 Va. Acts 1759.

42. VA. CODE §§ 18.2-152.1 to .14 (Supp. 1986).

unique problems posed by computer-assisted crimes, and although it does not contain some of the flaws that have marred other computer-assisted crime legislation, the Act still has some serious problems. In particular, the Act employs a vague definition of "computer," it still includes needless computer jargon, and it is replete with unnecessary and redundant penal sections. These problems, if not corrected, will seriously hamper the Act's effectiveness.

#### COMPUTER-RELATED DEFINITIONS IN THE VIRGINIA COMPUTER CRIMES ACT

The Act, like virtually every comprehensive computer-assisted crime statute,<sup>43</sup> begins with a glossary that defines the computer-related terms used throughout the statute.<sup>44</sup> Ideally, in addition to evidencing legislative intent, such a glossary should provide a comprehensive, yet flexible definition of "computer," and it should eliminate technical computer jargon, which is not helpful in defining offenses under the law. When necessary, the glossary also should broaden common law property definitions to include computer-related intangibles within the scope of property that can be the subject of larceny, embezzlement, and false pretenses. Judged by these standards, and set against the backdrop of analogous federal and state definitions, the Act generally improves upon the glossaries contained in the proposed federal computer crime legislation and in the state legislation based on the federal proposals. The Virginia Act's glossary falls far short of the ideal, however, because its definition of "computer" may be fatally vague, its definition of "computer program" is overly technical and confusing, and unnecessary computer jargon remains.

#### *The Definition of "Computer"*

The success of any computer-assisted crime statute depends upon its definition of "computer," because the meaning of this term delimits the statute's coverage. Unfortunately, this term also

---

43. See, e.g., S. 1766, 95th Cong., 1st Sess., 123 CONG. REC. 21,025 (1977) (proposed 18 U.S.C. § 1028(c)); ARIZ. REV. STAT. ANN. § 13-2301E (Supp. 1986); CAL. PENAL CODE § 502(a) (West Supp. 1986).

44. VA. CODE § 18.2-152.2 (Supp. 1986).

provides the legislature's greatest definitional challenge. As the House Committee on the Judiciary stated in 1984, "[t]he whole issue of defining the word 'computer' has plagued the consideration of computer crime legislation since its early days."<sup>45</sup> Even the computer industry cannot agree on a single meaning for "computer."<sup>46</sup> Ideally, the definition should be "broad enough to include nonelectronic computers . . . narrow enough to exclude a variety of electronic devices which rely on microprocessing circuitry . . . and flexible enough to cover technological advances."<sup>47</sup>

Early legislative attempts to define "computer" failed to meet this standard. For example, the first federal proposal defined "computer" as "an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes [all related equipment]."<sup>48</sup> Commentators criticized this definition both as overly narrow,<sup>49</sup> because it excluded sophisticated nonelectronic computers, and as overly broad,<sup>50</sup> because it included hand-held calculators, digital watches, and any other electronic devices fitted with microprocessors, even when those devices were not designed primarily for data processing functions.<sup>51</sup>

---

45. H.R. REP. NO. 894, 98th Cong., 2d Sess. 23, reprinted in 1984 U.S. CODE CONG. & AD. NEWS 3689, 3709.

46. *Computer Systems Protection Act of 1979*, S. 240: *Hearings Before the Subcomm. on Criminal Justice of the Senate Comm. on the Judiciary*, 96th Cong., 2d Sess. 5 (1980) (statement of Sen. Laxalt) [hereinafter cited as *Hearings*, S. 240]. Compare D. SPENCER, *COMPUTER DICTIONARY FOR EVERYONE* 50 (1979) (defining "computer" as "[a] device designed to execute a sequence of mathematical or logical operations automatically") with M. WEIK, *STANDARD DICTIONARY OF COMPUTERS AND INFORMATION PROCESSING* 79 (1969) (defining "computer" as "[a] device capable of solving problems by accepting data, performing prescribed operations on the data, and supplying the results of these operations") and C. SIPPL, *COMPUTER DICTIONARY* 44 (1966) (defining "computer" as "[a] device capable of accepting information, applying prescribed processes to the information, and supplying the results of these processes").

47. Roddy, *supra* note 12, at 361; see Gemignani, *supra* note 12, at 712.

48. S. 1766, 95th Cong., 1st Sess., 123 CONG. REC. 21,025 (1977) (proposed 18 U.S.C. § 1028(c)(2)). S. 240, the successor bill to S. 1766, contained the same definition. S. 240, 96th Cong., 1st Sess., 125 CONG. REC. 1190 (1979) (proposed 18 U.S.C. § 1028(c)(2)).

49. Roddy, *supra* note 12, at 361; Gemignani, *supra* note 12, at 708.

50. Gemignani, *supra* note 12, at 708.

51. Roddy, *supra* note 12, at 361 n.129 (calculators and digital wristwatches); Gemignani, *supra* note 12, at 708, 709 n.155 (electronic watches and automated traffic signals); see also *supra* note 11 (other devices fitted with microprocessing circuitry that the federal definition would consider "computers").

The commentators' complaint that the definition was overly broad should not be construed as a charge of unconstitutional overbreadth;<sup>52</sup> instead, it seems more properly a charge that the definition is too vague. Under the void for vagueness doctrine, enactments that prohibit certain activity may violate due process if they do not define the scope of that prohibition with adequate clarity. As the Supreme Court has noted:

It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined. . . . [B]ecause we assume that man is free to steer between lawful and unlawful conduct, we insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning.<sup>53</sup>

An illustration of the vagueness problems in many computer-assisted crime statutes is provided by the eighteen states that have adopted the early federal definition of "computer."<sup>54</sup> In seventeen

---

52. Overbreadth is a first amendment doctrine that courts use to invalidate laws that sweep within their prohibitions "activities that constitute an exercise of protected expressive or associational rights." L. TRIBE, *AMERICAN CONSTITUTIONAL LAW* § 12-24, at 710 (1978) (quoting *Thornhill v. Alabama*, 310 U.S. 88, 97 (1940)). According to Professor Tribe, a law may be void for overbreadth, on its face, if a significant portion of the law's target consists of protected activity and if the unconstitutional portions cannot be excised from the law in a single step. *Id.* at 711. Professor Tribe also notes that an otherwise valid law may be invalid for overbreadth, as applied, if it is enforced against protected activity. *Id.*

Typical computer-assisted crime statutes will pass both levels of overbreadth analysis. A court never could find a computer-assisted crime statute invalid for overbreadth on its face, because these laws do not target protected expression. Computer-assisted crime statutes also would not be invalid for overbreadth as applied, because they are enforced against conduct, not expression. Even the provision in computer-assisted crime statutes that arguably comes the closest to banning speech—the ban on mere unauthorized computer use, *see, e.g.*, COLO. REV. STAT. § 18-5.5-102(2) (1986); DEL. CODE ANN. tit. 11, § 932 (Supp. 1984)—does not prohibit protected expression. Instead, it bans theft of an item that facilitates expression—computer time and services. All agree that the government cannot prosecute a protester merely for airing his views. The government, however, can and should prosecute that individual for stealing a megaphone to amplify his voice, for breaking into a printshop to print his leaflets, or for using his employer's computer without authority to compose his speech. These prohibitions do not offend free speech values.

53. *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972).

54. ALASKA STAT. § 11.46.990(3) (Supp. 1986); ARIZ. REV. STAT. ANN. § 13-2301E(2) (1978 & Supp. 1986); COLO. REV. STAT. § 18-5.5-101(2) (1986); HAWAII REV. STAT. § 708-890 (Supp. 1984); IDAHO CODE § 18-2201(2) (Supp. 1986); IOWA CODE ANN. § 716A.1(2) (West Supp. 1986); MICH. COMP. LAWS ANN. § 752.792(2) (West Supp. 1986); MINN. STAT. ANN. § 609.87(3)

of these eighteen states, an individual who merely uses another's hand-held calculator without authorization can be prosecuted for a computer-assisted crime.<sup>55</sup> The public generally associates the term "computer" with more sophisticated data processors, and would not even begin to think of a hand-held calculator as a computer; yet the statutory definition in these jurisdictions does not dispel this perception by stating explicitly that, contrary to normal expectation, a calculator is a "computer."<sup>56</sup> As a result, the statutes proscribing unauthorized *computer* use in these states do not provide persons of ordinary intelligence with fair notice and warning that unauthorized *calculator* use is a crime, and thus these statutes should be considered void on vagueness grounds.

The Virginia General Assembly successfully addressed the criticism that the first federal definition of "computer" was overly narrow by defining "computer" as including any "electronic, magnetic, optical, hydraulic or organic" device.<sup>57</sup> The General Assembly

(West Supp. 1986); MONT. CODE ANN. § 45-2-101(8) (1985); NEV. REV. STAT. § 205.4735 (1986); N.M. STAT. ANN. § 30-16A-2(B) (1984); N.D. CENT. CODE § 12.1-06.1-01(3)(b) (1985); OHIO REV. CODE ANN. § 2913.01(M) (Page Supp. 1985); OKLA. STAT. ANN. tit. 21, § 1952(2) (West Supp. 1985); OR. REV. STAT. § 164.377(1)(b) (1985); R.I. GEN. LAWS § 11-52-1(B) (1981); TEX. PENAL CODE § 33.01(2) (Vernon Supp. 1986); WIS. STAT. ANN. § 943.70(1)(a) (West Supp. 1986).

55. See ALASKA STAT. § 11.46.200(a)(3) (Supp. 1986); ARIZ. REV. STAT. ANN. § 13-2316B (1978); COLO. REV. STAT. § 18-5.5-102(2) (1986); HAWAII REV. STAT. § 708-896 (Supp. 1984); IDAHO CODE § 18-2202(2) (Supp. 1986); IOWA CODE ANN. § 716A.2 (West Supp. 1986); MICH. COMP. LAWS ANN. § 752.795 (West Supp. 1986); MINN. STAT. ANN. § 609.89(1)(a) (West Supp. 1986); MONT. CODE ANN. § 45-6-311(1)(a) (1985); NEV. REV. STAT. § 205.4765(1)(d) (1986); N.M. STAT. ANN. § 30-16A-4 (1984); N.D. CENT. CODE § 12.1-06.1-08(2) (1985); OHIO REV. CODE ANN. § 2913.04 (Page 1982); OKLA. STAT. ANN. tit. 21, § 1953(4) (West Supp. 1985); OR. REV. STAT. § 164.377(4) (1985); R.I. GEN. LAWS § 11-52-3 (Supp. 1986); WIS. STAT. ANN. § 943.70(3)(a)(2) (West Supp. 1986).

The sole exception is Texas, which requires either that the unauthorized user breach a security system, TEX. PENAL CODE § 33.02 (Vernon Supp. 1986), or that the unauthorized user somehow harm the computer or computer data, *id.* § 33.03.

56. This logic applies with even greater force to digital watches, and to any electronic device that uses microprocessing circuitry solely to monitor performance or to time operations. Ordinary people simply do not consider these devices computers.

57. The definition reads, in full:

"Computer" means an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment,

included this phrase specifically to ensure that the definition "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. . . ." <sup>58</sup> The Virginia definition, however, remains open to a charge that it is overly broad. When read with reference to other terms in the glossary, for example, the Act's definition of "computer" includes a hand-held calculator: "an electronic . . . device which pursuant . . . to human instruction . . . can automatically perform [arithmetic functions] <sup>59</sup> . . . on [numbers] <sup>60</sup> and can communicate the results . . . to a person." <sup>61</sup> Consequently, in Virginia a person who willfully uses another's hand-held calculator without authority—that is, one who uses it intentionally and with a bad purpose—theoretically commits the crime of computer theft of services, a Class 1 misdemeanor. <sup>62</sup>

An ordinary person, however, usually does not consider hand-held calculators to be computers, and the Act's definition does not adequately inform such a person that calculators are "computers," for purposes of the Act, by stating explicitly that the definition covers these devices. As a result, unless the unauthorized calculator user had been able to discover that the Act covers calculators,

---

or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or device.

VA. CODE § 18.2-152.2 para. 1 (Supp. 1986). The Act separately defines "computer data," *id.* para. 2, "computer operations," *id.* para. 4, and "computer program," *id.* para. 5.

58. Burke, *Virginia's Response to Computer Abuses: An Act in Five Crimes*, 19 U. RICH. L. REV. 85, 93 (1984).

59. The Act includes "arithmetic functions" within its definition of "computer operations." VA. CODE § 18.2-152.2 para. 4 (Supp. 1986).

60. The Act includes "numbers" within its definition of "computer data," because a number can be a "representation of information, knowledge, facts, concepts or instructions which is being prepared or has been prepared and is intended to be processed . . . in a computer." *Id.* para. 2.

61. *See supra* note 57.

62. The Virginia computer theft of services statute provides: "Any person who willfully uses a computer or computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services, which shall be punishable as a Class 1 misdemeanor." VA. CODE § 18.2-152.6 (Supp. 1986). A Class 1 misdemeanor is punishable by "confinement in jail for not more than twelve months and a fine of not more than \$1,000, either or both." *Id.* § 18.2-11 (1982).

For a discussion of the willfulness requirement, see *infra* notes 227-28 and accompanying text.

by putting together the appropriate parts of three lengthy, complicated definitional sections,<sup>63</sup> that person could be charged with computer theft of services without any notice that unauthorized calculator use is prohibited by law. Admittedly, the individual acted with a bad purpose—that is, one that was morally improper—but moral impropriety alone does not make an act criminal. A law purporting to criminalize an act must provide “fair warning” so that “the person of ordinary intelligence [has] a reasonable opportunity to know what is prohibited,”<sup>64</sup> and so that criminal responsibility attaches only to acts that individuals “reasonably understand to be proscribed” by law.<sup>65</sup> Because the Virginia definition of “computer” does not provide “fair warning” to “the person of ordinary intelligence,” a vagueness challenge to the definition might be successful, although Virginia’s “willfulness” requirement does introduce an element of doubt that is not present with respect to the state statutes that employ the original federal definition of “computer.”

Even the mere possibility of vulnerability to a vagueness challenge is troublesome, however, because if someone were to succeed in challenging the definition of “computer” the entire Act would fail. The Act does contain a severability section designed to save provisions that “can be given effect without the invalid provision,”<sup>66</sup> but that section would not save the Act if the definition of “computer” were to be found invalid, because the definition is so interwoven with all of the Act’s remaining provisions that its invalidity would frustrate the legislative purpose in enacting computer-assisted crime legislation. A severability section merely reverses the presumption that the provisions of a statute comprise an inseparable whole and replaces it with a presumption of severability.<sup>67</sup> In this case, if the definition of “computer” were excised from

---

63. See *supra* notes 59-61 and accompanying text.

64. *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972); see *supra* note 53 and accompanying text.

65. See *supra* note 53 and accompanying text; *Flannery v. City of Norfolk*, 216 Va. 362, 365, 218 S.E.2d 730, 733 (1975) (quoting *Colten v. Kentucky*, 407 U.S. 104, 110 (1972), which, in turn, was quoting *United States v. Harriss*, 347 U.S. 612, 617 (1954)), *appeal dismissed*, 424 U.S. 936 (1976).

66. VA. CODE § 18.2-152.13 (Supp. 1986).

67. A statute will fail as a whole upon a finding that one provision is invalid, despite a severability provision, if the evidence adduces “the clear probability that the legislature

the Act due to invalidity, the presumption would be rebutted and the entire Act would fail, because every other provision in the Act depends upon the definition of "computer."

The Virginia General Assembly should make its intent clear. Most likely, the General Assembly did not intend the Act to target unauthorized calculator users, or users of other electronic devices that people generally do not think of as "computers," because the harm caused by unauthorized users of these devices is minimal and hardly worth the State's notice, and because the law should not punish such innocuous activity. If this is the case, the General Assembly should exclude calculators and other such devices from the definition of "computer."<sup>68</sup> On the other hand, if the General Assembly did intend to prohibit unauthorized use of such devices, the prohibition should be stated explicitly, to avoid a vagueness challenge.

The best alternative would be for the General Assembly to re-draft the definition of "computer" to incorporate, with modification, the improvements reflected in the definition first proposed in the Federal Computer Crime Prevention Act of 1983.<sup>69</sup> The

---

would not have been satisfied with the statute unless it had included the invalid part.' Whether the provisions are so interwoven that one being held invalid the others must fall, presents a question of statutory construction and of legislative intent." *Carter v. Carter Coal Co.*, 298 U.S. 238, 312-13 (1936) (quoting *Utah Power & Light Co. v. Pfost*, 286 U.S. 165, 184-85 (1932)); *Hannabass v. Maryland Cas. Co.*, 169 Va. 559, 571, 194 S.E. 808, 813 (1938) (quoting with approval *Carter Coal*).

68. In interpreting penal statutes, the courts have extended their prohibitions only to acts that not only are within the letter but also are within the spirit of the statute in question. See *Price v. Commonwealth*, 209 Va. 383, 386, 164 S.E.2d 676, 679 (1968) (quoting *McKinney v. Commonwealth*, 207 Va. 239, 243, 148 S.E.2d 829, 831-32 (1966)). Although this rule of interpretation might prevent application of the Act to users of calculators and other similar devices, the result would be much more certain if the General Assembly amended the Act to make clear its legislative intent.

The initial draft of the Virginia Computer Crimes Act did exclude hand-held calculators, but that exclusion was removed when opposition to a related limitation surfaced in the House. See *Burk*, *supra* note 58, at 90; *infra* note 78.

69. S. 1733, 98th Cong., 1st Sess., 129 CONG. REC. S11,448 (daily ed. Aug. 3, 1983); H.R. 1092, 98th Cong., 1st Sess., 129 CONG. REC. H219 (daily ed. Jan. 31, 1983) (companion bill to S. 1733). The definition reads, in full:

'[C]omputer' means an electronic, magnetic, optical, hydraulic, organic, or other *high speed data processing device or system* performing logical, arithmetic, or storage functions, and includes any property, data storage facility, or communications facility directly related to or operating in conjunction with such device or system; *but does not include an automated typewriter or type-*



limitations contained in this definition first exclude devices that usually are not considered "computers," by confining the term to high speed data processing devices or systems, and then exclude those high speed data processors that usually are not involved in computer-assisted crimes.<sup>70</sup> These limitations, if added to the Virginia definition of "computer" in the proper manner, would strengthen the Act significantly. First, the "high speed data processing device or system"<sup>71</sup> limitation could replace the extremely broad "device or group of devices" language contained in the Virginia definition of "computer,"<sup>72</sup> thereby excluding devices that use microprocessing circuitry primarily to monitor performance, to enhance performance, or to time operations, rather than to process data generally. This modification would exclude high-tech automobiles, dishwashers, refrigerators, microwave ovens, power tools, and other products designed to perform tasks that only incidentally involve data processing.<sup>73</sup> These devices simply do not belong within the coverage of a computer-assisted crime statute. On the other hand, this modification would not exclude other devices, such as automated teller machines (ATM's),<sup>74</sup> that are merely components of larger computer systems, because the Virginia Act still

---

*setter, a portable hand-held calculator, or 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.*

S. 1733, 98th Cong., 2d Sess., 129 CONG. REC. S11,448 (daily ed. Aug. 3, 1983) (proposed 18 U.S.C. § 1028(c)(1)) (emphasis added); H.R. 1092, 98th Cong., 2d Sess., 129 CONG. REC. H219 (daily ed. Jan 31, 1983) (proposed 18 U.S.C. § 1028(c)(1)) (emphasis added).

70. See *supra* note 69 (italicized portions). These exclusions first were proposed during consideration of S. 240 at the subcommittee level. *Hearings, S. 240, supra* note 46, at 2 (statement of Sen. Hatch).

Congress targeted four categories of computer-assisted crime: "First. The introduction of fraudulent records or data into the computer system; Second. The unauthorized use of computer related facilities; Third. The alteration or destruction of information or files[;] and Fourth. The stealing, whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable data." 125 CONG. REC. 1191 (1979) (statement of Sen. Ribicoff).

71. See *supra* note 69.

72. See *supra* note 57.

73. See *supra* notes 11 & 51 and accompanying text.

74. An automated teller machine contains microprocessing circuitry, but does not actually process data. An ATM receives data from the customer, transmits that data to the bank's central computer, receives instructions back from the central computer, and completes the customer's transaction by executing those instructions.

would include the phrase "related device[s and] equipment," which would encompass ATM's.<sup>75</sup> Second, the limitation enumerating specific devices not included in the definition of "computer" would exclude two categories of general data processing devices that are unlikely to be involved in computer-assisted crimes: first, automated typewriters, automated typesetters, and portable hand-held calculators,<sup>76</sup> which are manufactured to perform a single function and are not adaptable for general-purpose computing; and second, general-purpose computers "designed and manufactured for, and . . . used exclusively for, routine personal, family, or household purposes" that cannot interact with other computers, as installed.<sup>77</sup> This two-part limitation would cause the definition of "computer" to focus on only those computers likely to be involved in computer-assisted crimes: general-purpose computers used by governmental, educational, and commercial institutions; and general-purpose computers intended for personal, family, or household purposes that hackers can use to interact with other computers.

The Virginia General Assembly should adopt both limitations to the definition of "computer."<sup>78</sup> Before adopting the second limitation, however, Virginia should delete the phrase "designed and manufactured for" used in the proposed federal definition to

---

75. VA. CODE § 18.2-152.2 para. 1 (Supp. 1986) ("The term 'computer' includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.").

76. See *supra* note 69.

77. *Id.*

78. The first two versions of the Virginia Computer Crimes Act offered in the Virginia House of Delegates, H.B. 6, 1984 Sess., and H.B. 289, 1984 Sess., included both federal limitations. These limitations, however, were excised from later versions of the Act, see H.B. 6, 1984 Sess.; S. 347, 1984 Sess., ostensibly because the second limitation "placed too heavy a burden on the prosecution to prove that the computer involved was actually manufactured or used for a business purpose." Burk, *supra* note 58, at 90. This reasoning is curious; the General Assembly could have addressed most of its concern simply by deleting the phrase "designed and manufactured for" in the second limitation, which would make the purpose for manufacturing the computer irrelevant. See *infra* text accompanying note 79. The second portion of the General Assembly's concern, proving whether the computer had been used for a business purpose, actually would pose little concern. Because the only computers excluded by the second limitation would be computers installed in the home that could not interact with other computers, the only cases likely to arise involving such computers would be ones arising in a business context.

modify the exclusively "routine personal, family, or household" use exclusion. A computer designed and manufactured for business use, but used in the home for nonbusiness purposes, is no more likely to become the tool of a computer-assisted criminal than a computer designed specifically for home use. Irrespective of the use for which it was designed, a computer used exclusively for "personal, family, or household purposes," and incapable, as installed, of communicating with other computers, poses very little danger to society.<sup>79</sup> The "designed and manufactured for" phrase, therefore, unnecessarily restricts the home use exclusion, and Virginia should not adopt that phrase in its revised definition of "computer."

A redrafted definition of "computer," incorporating each of the preceding recommended changes, would read:

"Computer" means an electronic, magnetic, optical, hydraulic, or organic high speed data processing device or system which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or system, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve, or communicate computer programs, computer data, or the results of computer operations to or from a person, another computer, or another device; but does not include an automated typewriter or typesetter, a portable handheld calculator, or any computer which is used exclusively for routine personal, family, or household purposes and which is not used to communicate with or to manipulate any other computer.

### *The Use of Computer Jargon*

Because no computer-assisted crime statute can avoid using computer jargon completely, a legislature generally will define any unavoidable jargon in the statute's glossary.<sup>80</sup> If the legislature

---

79. *Accord* Burk, *supra* note 58, at 90 (noting that "[t]he 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").

80. *See, e.g.*, CAL. PENAL CODE § 502(a) (West Supp. 1986); FLA. STAT. ANN. § 815.03 (West Supp. 1986); N.J. STAT. ANN. § 2C:20-23 (West Supp. 1986).

uses jargon to define jargon, however, it defeats the goal of making the definitions understandable. The General Assembly drafted the Virginia Computer Crimes Act relatively free of computer jargon, but it could make the Act even better in this regard by revising the definition of "computer program"<sup>81</sup> and by eliminating every reference to "computer software."<sup>82</sup>

Most commentators criticized the excessive use of computer jargon in the proposed federal legislation, especially its use of the noun "access" as a verb<sup>83</sup> when the proper verb is "use." In response, several state statutes, including the Virginia Computer Crimes Act, substituted "use" for "access."<sup>84</sup> The Virginia Act defines computer "use" in terms of specific conduct: (1) causing a computer to perform or stop performing computer operations, (2) causing the withholding or denial of a computer's use to another user, or (3) causing another person to put false information into a computer.<sup>85</sup> The definition also includes any attempt to cause one of these three results.<sup>86</sup> This definition improves upon the federal definition by categorizing specific uses and by replacing technical terms with familiar words.<sup>87</sup>

---

81. VA. CODE § 18.2-152.2 para. 5 (Supp. 1986); see *infra* notes 88-92 and accompanying text.

82. VA. CODE § 18.2-152.2 para. 7 (Supp. 1986); see *infra* notes 93-96 and accompanying text.

83. Taber, *supra* note 12, at 537; see also Roddy, *supra* note 12, at 361 (criticizing the ambiguity of "access"). The definitional section of the proposed federal legislation provided: "'access' means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network." S. 1766, 95th Cong., 1st Sess., 123 CONG. REC. 21,025 (1977) (proposed 18 U.S.C. § 1028(c)(1)).

84. Colorado and Montana simply substituted the word "use" for "access," and retained the federal definition with only minor, nonmaterial changes. See COLO. REV. STAT. § 18-5.5-101(10) (1986); MONT. CODE ANN. § 45-6-310 (1985). Nevada and Wisconsin sidestepped the jargon problem by eliminating the definition of "access," and prohibiting willful, knowing, and unauthorized computer "use." NEV. REV. STAT. §§ 205.473 to .477 (1986); WIS. STAT. ANN. § 943.70 (West Supp. 1986). Virginia dropped "access" and defined "use." VA. CODE § 18.2-152.2 para. 12 (Supp. 1986).

85. VA. CODE § 18.2-152.2 para. 12 (Supp. 1986).

86. *Id.*

87. The federal definition of "access" also was criticized for being so broad that "it could include the use of almost anything having something to do with a computer." Gemignani, *supra* note 12, at 708. The Virginia definition of computer "use" likewise sweeps rather broadly. For example, disconnecting a computer will cause it to stop performing computer functions, failing to pay the computer owner might cause the withholding or denial of a

Although this definition significantly improves upon the proposed federal legislation, the General Assembly took a step backward when it defined "computer program" as "an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations."<sup>88</sup> Definitions should facilitate statutory enforcement and interpretation; they should not obfuscate and intimidate. To facilitate enforcement and interpretation of a computer-assisted crime statute, legislatures should define jargon with words that law enforcement authorities can understand easily, and not with mathematically technical phrases such as "an ordered set of data representing coded instructions or statements." Definitions that use familiar words and phrases are more workable and more understandable.

Montana's computer-assisted crime statute, which defines "computer program" as "an instruction or statement or a series of instructions or statements, in a form acceptable to a computer, that in actual or modified form permits the functioning of a computer or computer system and causes it to perform specified functions,"<sup>89</sup> improves on the Virginia definition not only in its use of familiar, less technical words, but also in two other respects. First, it recognizes that a computer program may consist of a single instruction or statement.<sup>90</sup> Second, by eliminating the word "coded," the definition leaves no doubt that a computer program written in any computer language will be "in a form acceptable to a computer,"

---

computer to another user, and inadvertently placing the wrong zip code on a computerized order form will cause another person to put false information into a computer. The Act's penal sections, however, require unauthorized computer use with the intent to commit some further act; therefore, the "users" enumerated above would commit no crime unless they possessed the intent to commit one of the proscribed acts. *See* VA. CODE §§ 18.2-152.3 to .7 (Supp. 1986).

88. VA. CODE § 18.2-152.2 para. 5 (Supp. 1986). Virginia borrowed most of this definition from GA. CODE ANN. § 16.9-92(4) (1984). Burk, *supra* note 58, at 93 n.37.

89. MONT. CODE ANN. § 45-2-101(10) (1985).

90. The Department of Justice made a similar suggestion with respect to the first proposed federal legislation. 125 CONG. REC. 1194 (1979) (statement of John C. Keeney, Acting Ass't Att'y Gen., Crim. Div.). That suggestion was incorporated in the next version of the Federal Computer Systems Protection Act. S. 240, 96th Cong., 1st Sess., 125 CONG. REC. 1191 (1979) (proposed 18 U.S.C. § 1028(c)(8)).

even if it is a paper copy of the program.<sup>91</sup> Consequently, Virginia should consider adopting the Montana definition, but in a slightly modified form: "‘Computer program’ means one or more related instructions or statements, composed and structured in a form acceptable to a computer, that, when executed by a computer in actual or modified form, cause it to perform one or more computer operations."<sup>92</sup>

The Act also suffers from its use of the computer jargon term "computer software,"<sup>93</sup> which the Act defines as "a set of computer programs and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network."<sup>94</sup> The Virginia General Assembly should replace this definition with an addendum to the definition of "computer program," providing: "‘Computer program’ shall include all associated procedures and documentation." Although two of the Act’s penal sections apply to "computer software,"<sup>95</sup> both of these

91. A paper copy of a computer program would fit the Montana definition because, once "modified" by entry into the memory of a computer, it will permit the computer to perform specified functions. *See supra* text accompanying note 89. Under the Virginia definition, on the other hand, instructions and statements might not be considered "coded" until they have been stored either in the internal or external memory of a computer.

92. "Computer operation" already is defined in the Virginia Act as "arithmetic, logical, monitoring, storage or retrieval functions and any combinations thereof, [including], but . . . not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses [or] for a particular computer . . . a function for which that computer was generally designed." VA. CODE § 18.2-152.2 para. 4 (Supp. 1986).

93. One expert in the field observed at hearings on the first federal proposal: "[T]he term ‘software’ should not be used because it is a jargon word that has several different meanings. . . ." *Hearings, S. 1766, supra* note 23, at 54.

94. VA. CODE § 18.2-152.2 para. 7 (Supp. 1986). The model for this definition was ARIZ. REV. STAT. ANN. § 13-2301 (1978). Burk, *supra* note 58, at 93 n.37.

95. VA. CODE §§ 18.2-152.4, .8 (Supp. 1986). Section 18.2-152.4, which prohibits "computer trespass," provides, in pertinent part:

Any person who uses a computer or computer network without authority and with the intent to:

1. Temporarily or permanently remove computer data, computer programs or *computer software* from a computer or computer network;

. . . .

3. Alter or erase any computer data, computer programs or *computer software*;

. . . .

sections also apply to computer programs.<sup>96</sup> Thus, these references also should be deleted. These changes would simplify and clarify the Act without affecting its scope.<sup>97</sup>

### *The Definition of "Property"*

The 1977 Virginia Supreme Court decision in *Lund v. Commonwealth*,<sup>98</sup> in which the court held that unauthorized use of computer time and services could not constitute either grand larceny or false pretenses under existing Virginia statutes because time and services were not "property,"<sup>99</sup> posed a great obstacle to successful computer-assisted theft prosecution in Virginia. Because of the magnitude of this problem, the General Assembly effectively overruled *Lund* just one year later when it enacted Virginia's first

---

6. Make or cause to be made an unauthorized copy . . . of computer data, computer programs or *computer software* . . . shall be guilty of the crime of computer trespass. . . .

*Id.* § 18.2-152.4 (emphasis added). Section 18.2-152.8, which enumerates the "property capable of embezzlement," provides, in pertinent part: "For purposes of § 18.2-111, personal property subject to embezzlement shall include . . . [f]inancial instruments, computer data, computer programs, [and] *computer software*. . . ." *Id.* § 18.2-152.8 (emphasis added).

96. See *supra* note 95.

97. The complete definition of "computer program," as modified, would read:

'Computer program' means one or more related instructions or statements, composed and structured in a form acceptable to a computer, that, when executed by a computer in actual or modified form, cause it to perform one or more computer operations. The term 'computer program' shall include all associated procedures and documentation.

98. 217 Va. 688, 232 S.E.2d 745 (1977). Lund, a graduate student at Virginia Polytechnic Institute, had been convicted of grand larceny for the theft of "keys, computer cards, computer printouts and [for] using 'without authority computer operation time and services of [the university] . . . with intent to defraud.'" *Id.* at 688-89, 232 S.E.2d at 746. Specifically, Lund had been charged with larceny, VA. CODE § 18.2-100 (1950) (reenacted in 1975 as § 18.2-95), and false pretenses, VA. CODE § 18.2-118 (1950) (reenacted in 1975 as § 18.2-178).

99. 217 Va. at 691-92, 232 S.E.2d at 748. Specifically, the court held that only the "goods and chattels of another" could be the subject of larceny, and that "goods and chattels" did not include computer time and services. Another reason that unauthorized computer use could not be the subject of larceny, according to the court, was that the Virginia Code also required "a taking and carrying away of a certain concrete article of personal property." The court also concluded that time and services could not be the subject of false pretenses at common law because neither could be carried away. The court supported these conclusions by noting that, although some jurisdictions had amended their criminal codes to include time and services, Virginia had not. *Id.*

computer-assisted crime statute.<sup>100</sup> The 1978 statute stated explicitly that "[c]omputer time or services or data processing services or information or data stored in connection therewith" was property that could be the subject of larceny, embezzlement, or false pretenses.<sup>101</sup> The Virginia General Assembly repealed this statute when it passed the Virginia Computer Crimes Act in 1984,<sup>102</sup> but it retained the language of the earlier statute as the definition of "computer services,"<sup>103</sup> and it included the term "computer services" in the definition of "property,"<sup>104</sup> thus achieving the same result.<sup>105</sup>

The General Assembly further broadened the Act's definition of "property" by including within it three other classes of property that were not the subject of larceny at common law: real property,<sup>106</sup> financial instruments,<sup>107</sup> and computer data and programs.<sup>108</sup> In addition, the Act states that computer-related

---

100. Act of Apr. 8, 1978, ch. 686, 1978 Va. Acts 1120 (codified at VA. CODE § 18.2-98.1 (1982)) (repealed 1984).

101. *Id.*

102. Act of Apr. 11, 1984, ch. 751, § 2, 1984 Va. Acts 1759, 1763.

103. VA. CODE § 18.2-152.2 para. 6 (Supp. 1986).

104. *Id.* para. 11(4). The definition provides, in full:

"Property" shall include:

1. Real property;
2. Computers and computer networks;
3. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
  - a. Tangible or intangible;
  - b. In a format readable by humans or by a computer;
  - c. In transit between computers or within a computer network or between any devices which comprise a computer; or
  - d. Located on any paper or in any device on which it is stored by a computer or by a human; and
4. Computer services.

*Id.* para. 11.

105. See Burk, *supra* note 58, at 95 (asserting that the inclusion of "computer services" in the definition of "property" was in response to Lund).

106. VA. CODE § 18.2-152.2 para. 11(1) (Supp. 1986). Real property was excluded at common law because it could not be carried away. R. PERKINS & R. BOYCE, *supra* note 21, at 292. Furthermore, a person who stole a real estate deed did not commit larceny at common law because a document merged with the object it represented. *Id.* at 295.

107. VA. CODE § 18.2-152.2 para. 11(3) (Supp. 1986). Negotiable notes and bills were excluded at common law. R. PERKINS & R. BOYCE, *supra* note 21, at 295.

108. VA. CODE § 18.2-152.2 para. 11(3) (Supp. 1986). Computer data and programs were excluded at common law because they represented intangible property—information and



intangibles are "property" even when they are not readable by humans, are in transit between computers, or are stored within a computer.<sup>109</sup> Taken together, the Act's definitions of "computer services" and "property" achieve the General Assembly's objective by removing the obstacles to conviction created by this portion of the decision in *Lund*.

### *Recommendations*

Although the glossary in the Virginia Computer Crimes Act improves upon the comparable provisions of the early proposed federal legislation and nearly every other state computer crime statute, and even though it successfully broadens the definition of "property" to allow effective prosecution of computer-assisted crimes, it remains unsatisfactory in two respects. First, the definition of "computer" fails to exclude devices that ordinary persons do not consider computers and devices that cannot be used to commit crimes contemplated by the Act. Second, the General Assembly has not resolved the jargon problem; the Act contains unnecessary references to "computer software" and the definition of "computer program" is overly technical. The Act will not become a truly workable response to computer-assisted crime until refinements along the lines of those recommended in this Note have been made to the Act's glossary.

### THE PROSCRIPTIONS IN THE VIRGINIA COMPUTER CRIMES ACT

The Virginia Computer Crimes Act proscribes a wide range of computer-assisted activities, including unauthorized use of a computer with the intent (1) to obtain property or services by false pretenses, or to embezzle, commit larceny, or convert the property of another;<sup>110</sup> (2) to remove, alter, or erase computer data, com-

---

knowledge—and intangibles were not subjects of larceny at common law. R. PERKINS & R. BOYCE, *supra* note 21, at 295. To illustrate, if a computer tape containing extremely valuable information were stolen, the common law would not recognize the information contained on the tape. The defendant could be tried only for the larceny of the physical object, and the value of the tape itself might be so slight that only a charge of petit larceny would lie. *Accord Lund*, 217 Va. at 692, 232 S.E.2d at 748. *But see infra* notes 135-47 and accompanying text (criticizing the test of "actual value" in *Lund*).

109. VA. CODE § 18.2-152.2 para. 11(3)(a)-(c) (Supp. 1986).

110. *Id.* § 18.2-152.3.

puter programs, or computer software from a computer;<sup>111</sup> (3) to cause a computer to malfunction or to cause physical injury to the property of another;<sup>112</sup> (4) to create or alter a financial instrument or effect an electronic transfer of funds;<sup>113</sup> (5) to examine any employment, salary, credit, or any other financial or personal information relating to any other person;<sup>114</sup> (6) to obtain computer services;<sup>115</sup> or (7) to cause physical injury to an individual.<sup>116</sup> The Act also proscribes using a computer as an instrument of forgery.<sup>117</sup> In short, the Act prohibits virtually every act of an *unauthorized* computer user.<sup>118</sup> This section examines these prohibitions to determine whether they adequately address the conduct that the General Assembly sought to proscribe and whether they unnecessarily duplicate either pre-existing statutes or each other.

### *Computer Fraud*

The first of the Act's enumerated crimes is "computer fraud," which prohibits unauthorized computer use with the intent to commit the traditional property crimes of false pretenses, larceny, embezzlement, or conversion.<sup>119</sup> The Commonwealth must prove four elements to obtain a conviction for computer fraud: first, that the defendant used a computer; second, that the defendant's use was without authority; third, that the defendant intended to com-

---

111. *Id.* § 18.2-152.4.1, .4.3.

112. *Id.* § 18.2-152.4.2, .4.5.

113. *Id.* § 18.2-152.4.4.

114. *Id.* § 18.2-152.5.

115. *Id.* § 18.2-152.6.

116. *Id.* § 18.2-152.7.

117. *Id.* § 18.2-152.14.

118. All but one of the Act's penal sections expressly prohibit conduct only when the perpetrator acts "without authority." See *id.* §§ 18.2-152.3 to .7. The phrase "without authority" is unnecessary in the section forbidding use of a "computer as instrument of forgery," *id.* § 18.2-152.14, because a forger by definition acts without authority.

119. The computer fraud section provides:

Any person who uses a computer or computer network without authority and with the intent to:

1. Obtain property or services by false pretenses;
2. Embezzle or commit larceny; or
3. Convert the property of another shall be guilty of the crime of computer fraud. . . .

*Id.* § 18.2-152.3.

mit one of the enumerated crimes; and fourth, that the value of the property or services the defendant obtained met the threshold value for a felony or misdemeanor.<sup>120</sup> Because the Act's expanded definition of "property"<sup>121</sup> applies to any crime mentioned in the Act, the Commonwealth need not prove that the property obtained could have been the subject of false pretenses, larceny, embezzlement, or conversion as those crimes are defined under Virginia common law.

The first element of computer fraud requires proof that the defendant used a computer. In proving this element, the Commonwealth faces the definitional problems with the terms "computer" and "use" discussed previously.<sup>122</sup> Further analysis of these definitions is unnecessary, but the remaining elements of computer fraud need additional examination.

The second element of computer fraud requires proof that the defendant's use was "without authority." According to the Act, a person uses a computer without authority "when he has no right or permission of the owner to use a computer, or, he uses a computer in a manner exceeding such right or permission."<sup>123</sup> If a prosecutor were to attempt to prove this element without reference to the other elements of computer fraud, that prosecutor first would have to determine whether the owner had given the defendant the express or implied right or permission to use the computer. If so, the prosecutor then would have to determine whether the defendant's use had exceeded that right or permission. While the prosecutor often would be able to carry this burden with a minimum amount of evidence, the two-step authority inquiry could pose an insurmountable obstacle in some cases, especially those arising in a business context, because many businesses do not have well-defined rules governing employee computer use.<sup>124</sup>

---

120. *See id.*

121. *See supra* note 104.

122. *See supra* notes 45-79 and accompanying text ("computer"); notes 83-87 and accompanying text ("use").

123. VA. CODE § 18.2-152.2 para. 13 (Supp. 1986).

124. *Cf. Burk, supra* note 58, at 96 ("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.").

Fortunately, the authority element need not be analyzed in isolation. A settled rule of criminal law<sup>125</sup> holds that "[n]o man can authorize another to do what he may not lawfully do himself. If the attempt to confer such authority be made, and the unlawful act be done, both are guilty."<sup>126</sup> Under this rule, proof that the defendant used the computer intending to commit one of the object crimes also constitutes proof that the defendant's use was without authority. A claim by the defendant that the owner authorized the use will not relieve the defendant of criminal responsibility; it merely will tend to indicate the owner's involvement in criminal activity. In essence, this rule authorizes analysis of the authority element in conjunction with the third element of computer fraud, which requires the defendant to use a computer "with the intent" to obtain property or services by false pretenses, or to commit larceny, embezzlement, or conversion.<sup>127</sup> Analyzed in this manner, the difficulty associated with the authority element disappears and the focus shifts to the element of intent.

The intent element has problems of its own, stemming from the list of crimes enumerated in the computer fraud section.<sup>128</sup> By forcing the Commonwealth to prove that the defendant used the computer without authority with the specific intent to obtain property or services by false pretenses, or to commit larceny, embezzlement, or conversion, the statute requires the prosecutor to decide not only which one of these crimes applies to the particular facts of the case, but also whether the defendant intended to commit that particular crime. Fortunately, the General Assembly has eased the prosecutor's burden in proving the elements of the particular crime by including in the Act the broad definition of the property that may be the subject of the crime.<sup>129</sup> Because of this broad definition, the crime of computer fraud encompasses unauthorized com-

---

125. See 22 C.J.S. *Criminal Law* § 39 (1961).

126. *State v. Henaghan*, 73 W. Va. 706, 713, 81 S.E. 539, 542 (1914), *overruled on other grounds*, *State v. Bragg*, 140 W. Va. 585, 87 S.E.2d 689 (1955).

127. See VA. CODE § 18.2-152.3 (Supp. 1986); *supra* note 119. These enumerated crimes are defined elsewhere in the Virginia Code. See *id.* § 18.2-178 (1982) (false pretenses); *id.* § 18.2-95 (larceny); *id.* § 18.2-111 (embezzlement); *id.* § 18.2-115 (Supp. 1986) (conversion).

128. See *supra* note 127 and accompanying text.

129. See *supra* note 104.

puter use with the intent to acquire almost any type of property, tangible or intangible.

The final element of computer fraud hinges on the Commonwealth's decision whether to charge the defendant with a felony or with a misdemeanor—a decision that depends on whether the value of the property obtained meets the \$200 threshold value for a felony. Unfortunately, the language of the threshold provision, which terms that underlying offense a felony “[i]f the value of the property or services obtained is \$200 or more” and a misdemeanor if “the value of the property or services obtained is less than \$200,”<sup>130</sup> raises two serious questions. First, if the prosecutor charges the defendant with a misdemeanor and cannot prove that the defendant actually *obtained* any property or services, can the penalty provision support the interpretation that the defendant's unauthorized computer use constituted computer fraud? Second, if the prosecutor charges the defendant with a felony, and the market value of the property or services taken cannot be determined, how should the court measure the actual value of the property or services?

The first question arises from a possible judicial construction of the words “property or services obtained” in the penalty provision of the computer fraud section.<sup>131</sup> A court could construe these words as excluding defendants who fail to “obtain” any property or services, regardless of their intent, while including defendants who do obtain property or services, even if the property or services has little or no value. This construction incorrectly shifts the focus of the computer fraud section from the defendants' fraudulent conduct to whether they successfully accomplished the object crime. By exonerating defendants who try to use a computer to obtain property or services but do not succeed, this construction essentially redefines computer fraud from use of a computer without authority *in an effort* to commit the object crime to use of a computer without authority *actually* to commit the object crime.

This “no property, no crime” interpretation ignores the “with the intent” language of the computer fraud section.<sup>132</sup> That phrase,

---

130. VA. CODE § 18.2-152.3.3 (Supp. 1986).

131. *Id.*

132. *Id.*

together with the title of the section itself, "computer fraud," evidences the General Assembly's intent to proscribe the *fraud* committed by a person who uses a computer without authority with the intent to commit certain crimes, and not just to reenact the object crimes in a new form. In other words, the General Assembly wanted to define a *new* crime, not to redefine existing crimes committed by using a computer.<sup>133</sup> Focusing on this legislative intent, courts should construe the penalty provision of the computer fraud section as including perpetrators who do not complete the object crime because they fail to obtain the coveted property. Courts should convict such perpetrators of misdemeanor computer fraud.<sup>134</sup>

The second question involves the trouble courts have had in computing the market value of computer-related intangibles such as the contents of a computer program or data file. The Virginia Supreme Court took a narrow-minded view of this issue in *Lund*, when it rejected the Commonwealth's argument that the measure of the value of computer printouts seized from the defendant should be the cost of the labor and services required to produce them.<sup>135</sup> The court stated that, in the absence of evidence about a stolen article's market value, the proper measure is the actual value of the article.<sup>136</sup> Because the computer center director had testified that the printouts were no more valuable than scrap paper, the court held that the evidence of value was insufficient to convict the defendant of grand larceny.<sup>137</sup>

This measure of value has little validity in a modern world. "Actual value" no longer means just the cost of materials; computer programs and data files have little worth when so measured. The information contained in computerized files, and the competitive

---

133. *Accord* Burk, *supra* note 58, at 91 (asserting that one of the General Assembly's goals was to "treat the proscribed activities as *new* crimes rather than as existing crimes" (emphasis in original)); *id.* at 96 (asserting that "computer fraud" is a "new [crime] not found elsewhere in the Virginia Code").

134. An intent-based construction also would fulfill the rule of construction that, "[i]n construing a statute, every word in it must be given its full effect, if that can be done consistently." 17 MICHIE'S JURISPRUDENCE *Statutes* § 42, at 326 (1979).

135. 217 Va. at 692, 232 S.E.2d at 748.

136. *Id.* at 692-93, 232 S.E.2d at 748.

137. *Id.* at 693, 232 S.E.2d at 748.

edge gained by a company that can use those files, supply the real value. Simply put, information means money in today's society.

In a later case, *Evans v. Commonwealth*,<sup>138</sup> the Virginia Supreme Court hinted that it might be willing to apply an actual value test that would better approximate the true value of computer programs and data files. In *Evans*, which involved a defendant who had taken a computer-generated "customer security list" from his employer, the Commonwealth reduced a charge of grand larceny to petit larceny,<sup>139</sup> evidently because of the uncertainty in calculating the market value of the list. This tactic paid off for the Government because, although the court quoted the "actual value" language in *Lund*,<sup>140</sup> the court was able to affirm the defendant's petit larceny conviction on the ground that petit larceny only requires proof that the article taken has some minimal value; it does not require proof of a *specific* value.<sup>141</sup> Significantly, although the court could have based its decision on the actual value of the paper,<sup>142</sup> it relied instead on evidence showing that a competitor had used the stolen list, which indicated that the competitor had found the information in the list valuable, and on testimony that the list was an invaluable sales tool.<sup>143</sup> The court concluded from this evidence that the list had value apart from that of the paper.<sup>144</sup>

The court's conclusion in *Evans* accorded with *Hancock v. Texas*,<sup>145</sup> in which the Texas Supreme Court held that a court may consider the value of a computer program to the victim's competitors and clients in determining the value of that computer program in a theft prosecution.<sup>146</sup> The Virginia judiciary should apply this test of actual value not only in a case such as *Evans*, but also in any case involving the theft of computer programs, data files, or

---

138. 226 Va. 292, 308 S.E.2d 126 (1983).

139. *Id.* at 294 n.1, 308 S.E.2d at 127 n.1.

140. *Id.* at 297, 308 S.E.2d at 129 (quoting *Lund*, 217 Va. at 692, 232 S.E.2d at 748).

141. *Id.*

142. Although the value of the paper was mere pennies, that value would have sustained a petit larceny conviction. See *supra* note 141 and accompanying text.

143. 226 Va. at 297, 308 S.E.2d at 129.

144. *Id.* One copy of the list had been supplied to a competing bank. *Id.* at 295, 308 S.E.2d at 128.

145. 402 S.W.2d 906 (Tex. Crim. App. 1966).

146. *Id.* at 909-11.

other property valued primarily for the information it contains. The computer fraud section then would give law enforcement officials and prosecutors a powerful weapon against computer-assisted theft.<sup>147</sup>

### *Computer Trespass*

The single offense of "computer trespass" actually consists of using a computer without authority with the intent to cause one of six possible results: (1) temporarily or permanently removing information in various forms from a computer; (2) causing a computer to malfunction; (3) altering or erasing information contained in a computer; (4) "[effecting] the creation or alteration of a financial instrument or of an electronic transfer of funds"; (5) "causing physical injury to the property of another"; and (6) making an unauthorized copy of computer data or programs.<sup>148</sup> Because these intended results appear to have little in common beyond the requirement that the perpetrator attempt to achieve them while using a computer without authority, each must be discussed separately.

### *Intent to Remove Computer Information*

The first portion of the computer trespass section involves using a computer without authority with the intent "[t]emporarily or permanently [to] remove computer data, [or] computer programs . . . from a computer or computer network."<sup>149</sup> Although this provision bears a striking substantive similarity to the computer fraud section,<sup>150</sup> it differs in three important respects. First, this portion of the computer trespass section relieves the Commonwealth of the

---

147. Another alternative would be to include a statutory test of value in the Act's glossary that would direct the courts to determine value based on the value to the owner, any other user of the computer, the offender, or any third party affected by the offense, whichever is greatest. Burk, *supra* note 58, at 97.

148. VA. CODE § 18.2-152.4 (Supp. 1986). Computer trespass is punishable as a Class 1 misdemeanor. *Id.*

149. *Id.* § 18.2-152.4.1. All references to "computer software" are omitted throughout the discussion of computer trespass because this jargon term should be deleted from the Act. See *supra* notes 93-97 and accompanying text.

150. Compare *supra* text accompanying note 149 (portion of computer trespass section) with *supra* note 119 (computer fraud section).



burden of proving either that the defendant intended to deprive the property owner of possession permanently, as the Commonwealth is required to do to prove computer fraud with the intent to commit larceny or false pretenses,<sup>151</sup> or that the defendant intended to misappropriate property already in the defendant's possession, as the Commonwealth is required to do to prove computer fraud with the intent to commit embezzlement or conversion.<sup>152</sup> In a prosecution under this portion of the computer trespass section, the Commonwealth will meet its burden of proof if it proves that the defendant intended to remove the property from the computer even temporarily,<sup>153</sup> and the issue of whether the defendant had "possession" of the property prior to removing it from the computer will be irrelevant. Second, the prosecutor need not prove that the property the defendant intended to acquire had value, as probably would be required in a prosecution for computer fraud.<sup>154</sup> As a result, when the prosecutor is unsure whether the property the defendant intended to obtain had value, the better charge is computer trespass, not computer fraud.<sup>155</sup> Third, the General Assembly limited the scope of this provision to computer-related intangible property.<sup>156</sup> The computer fraud section, on the other hand, contains no such limitation.<sup>157</sup>

The computer-related intangibles limitation may reflect a legislative desire to relieve the Commonwealth of the burden of proving value and permanent deprivation only when the property involved

---

151. For example, because the Virginia definition of "larceny" requires the "wrongful taking of personal goods of some intrinsic value, belonging to another, without his assent, and with the intention to deprive the owner thereof permanently," *Skeeter v. Commonwealth*, 217 Va. 722, 725, 232 S.E.2d 756, 758 (1977) (quoting *Dunleavy v. Commonwealth*, 184 Va. 521, 524, 35 S.E.2d 763, 764 (1945)), a prosecutor charging computer fraud with the intent to commit larceny, VA. CODE § 18.2-152.3.2 (Supp. 1986), must prove that the defendant had intended to deprive the owner of possession permanently.

152. See R. PERKINS & R. BOYCE, *supra* note 21, at 356-57.

153. See *supra* text accompanying note 149.

154. The better interpretation with respect to computer fraud is that the prosecutor must prove that the defendant at least *intended* to obtain something of value, although the prosecutor need not prove that the defendant *actually* obtained anything of value. See *supra* notes 131-134 and accompanying text.

155. This choice also avoids the issue of how to measure the value of computer-related property, which remains uncertain in Virginia. See *supra* notes 135-47 and accompanying text.

156. See *supra* text accompanying note 149.

157. See *supra* note 119.

falls within this unique category. Within its ambit, however, this portion of the computer trespass section provides an important weapon against computer-assisted crime, as the first two differences between this provision and the computer fraud section demonstrate. The relaxed burden of proof demonstrated by these two differences evidences a legislative willingness to depart from Virginia's conservative common law tradition regarding crimes against property in order to provide increased protection against crimes involving computer-related property.

### *Intent to Cause a Computer to Malfunction*

The second portion of the computer trespass section involves unauthorized computer use with the intent to cause a computer to malfunction.<sup>158</sup> This provision does not apply to physical attacks on a computer, such as bombing or shooting it;<sup>159</sup> the provision applies solely to using a computer with the intent to cause a computer malfunction. Physical attacks on computers constitute malicious mischief,<sup>160</sup> not computer trespass.

Even situations that do fall within the scope of this computer trespass provision often are better charged as other crimes. For example, if an unauthorized computer user succeeds in causing a computer malfunction, and that malfunction damages the computer, the proper charge still is malicious mischief.<sup>161</sup> Moreover, if an unauthorized computer user succeeds in causing a malfunction

---

158. Read in conjunction with the rest of the computer trespass section, the provision states: "Any person who uses a computer . . . without authority and with the intent to . . . [c]ause a computer to malfunction regardless of how long the malfunction persists . . . shall be guilty of the crime of computer trespass. . . ." VA. CODE § 18.2-152.4 (Supp. 1986).

159. See D. PARKER, *supra* note 13, at 18; T. WHITESIDE, *supra* note 12, at 4; Gemignani, *supra* note 12, at 682 & n.7.

160. VA. CODE § 18.2-137 (1982) ("If any person, unlawfully, but not feloniously . . . destroy, deface or injure any property, real or personal, not his own . . . he shall be guilty of a Class 1 misdemeanor."). The perpetrator also might be chargeable under section 18.2-121, which prohibits "ent[ry of] the land . . . or . . . building of another for the purpose of damaging such property or any of the contents thereof or in any manner to interfere with the rights of the owner, user, or the occupant thereof to use such property free from interference, *id.* § 18.2-121, or under section 18.2-81, which prohibits burning or destroying personal property by explosive device, *id.* § 18.2-81, depending on the facts of the case.

161. See 12A MICHIE'S JURISPRUDENCE *Malicious Mischief* § 3 (1978) (noting that malicious mischief applies to any such injury that "impair[s] the utility or diminish[es] the value of [the] property [affected]").

that does not damage the computer physically, that user almost certainly would have caused the malfunction either by erasing or altering computer data<sup>162</sup> or programming instructions,<sup>163</sup> which would be a violation of the third provision of the computer trespass section.<sup>164</sup> Consequently, the second provision of the computer trespass section extends the coverage of the Virginia Code only to the extent that it covers malfunctions that do not result in physical damage to the computer and that are not the result of alteration or erasure of computer data or programming instructions. Such malfunctions likely would be difficult to detect, and evidence of these crimes likely would be scant. As a practical matter, therefore, this portion of the computer trespass section should be considered a relatively useless provision that should provide the basis for few, if any, prosecutions.

### *Intent to Alter or Erase Computer Information*

The third portion of the computer trespass section proscribes unauthorized computer use "with the intent to . . . [a]lter or erase any computer data [or] computer programs."<sup>165</sup> The General Assembly apparently designed this offense to snare "hackers," computer enthusiasts who use their computers to break into governmental, educational, or commercial computer systems.<sup>166</sup> Many of these "computer raiders"<sup>167</sup> consider trying to outwit a computer's security system just a game,<sup>168</sup> and often boast of their accomplish-

---

162. The Act defines "computer data" as "any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network." VA. CODE § 18.2-152.2 para. 2 (Supp. 1986).

163. "Programming instructions" are simply computer data assembled into computer-readable instructions. One or more of these instructions make up every "computer program." See *id.* para. 5 (definition of "computer program"); see also *supra* notes 88-92 and accompanying text (discussing how to improve the definition).

164. See *infra* note 165 and accompanying text.

165. VA. CODE § 18.2-152.4 (Supp. 1986).

166. See, e.g., *Milwaukee Discovers 'WarGamesmanship'*, NEWSWEEK, Aug. 22, 1983, at 22.

167. *Id.*

168. One survey of college computer science students revealed that "34 per cent had tried to penetrate the security of the [school's] system." 125 CONG. REC. 31,167 (1979) (quoting an article in *Canadian Business* by Lydia Dotto). The survey concluded: "Many of the students believed they weren't doing anything wrong, unless they were harming an identifiable

ments by "publishing" the systems' passwords and access codes in computer "bulletin boards."<sup>169</sup> This practice forces victimized organizations to reprogram their computers with increasingly sophisticated and more costly security systems.

This portion of the computer trespass section, however, does not address much of this mischief, because these hackers often do not erase or alter data; they merely peruse information contained in the computers' memory. These individuals commit computer invasion of privacy or theft of services,<sup>170</sup> not computer trespass. The third portion of the computer trespass section is aimed at a different breed of hacker—the computer vandal who not only penetrates the computer's security system, but also alters or erases information contained in the computer's files<sup>171</sup>—and for this purpose it likely will be highly effective.

The Commonwealth also should consider using this provision as a supplemental charge to computer fraud if the defendant allegedly used a computer with the intent to commit larceny, embezzlement, false pretenses, or conversion, or as a supplemental charge to malicious mischief if the defendant used a computer with the intent to cause a computer malfunction. These crimes are virtually impossible to commit by computer *without* alteration or erasure of some form of computer data or programming instructions.<sup>172</sup> Charging computer trespass in these instances gives the prosecutor a fallback charge upon which to base a conviction.

---

individual. Cheating a large organization didn't seem to count." *Id.* The survey also revealed "a high correlation between [computer] competence and an inclination to engage in questionable behavior—probably because of the challenge involved." *Id.*

169. See *supra* note 9.

170. VA. CODE § 18.2-152.5 (Supp. 1986) (computer invasion of privacy); *id.* § 18.2-152.6 (theft of services); see *infra* notes 206-35 and accompanying text.

171. For examples of such instances, see 130 CONG. REC. S1179 (daily ed. Feb. 8, 1984) (remarks of Sen. Cohen) (reporting actions of hackers who broke into a credit bureau computer and changed records of prominent persons); Dobbins, *Watch Out Roscoe, Susan Thunder, et al.: Computer Criminals Get Caught*, Baltimore Sun, June 6, 1983, at —, col. — (reprinted in 129 CONG. REC. E2708 (daily ed. June 6, 1983)) (reporting how hackers gained access to computerized patient records and doubled patients' medication dosages).

172. See Burk, *supra* note 58, at 86-87.

*Intent to Create or Alter a Financial Instrument or Electronic Fund Transfer*

The fourth portion of the computer trespass section prohibits unauthorized computer use with the intent to create or alter a financial instrument or to effect an electronic transfer of funds.<sup>173</sup> This provision undoubtedly was intended to address the very real concerns of the banking industry about computer-assisted crime.<sup>174</sup> Indeed, the impetus for drafting the Virginia Computer Crimes Act was a request from the Virginia League of Savings Institutions,<sup>175</sup> and the definition of "financial instrument" was drafted explicitly to ensure "that automated teller machine transactions are protected by [the] Act."<sup>176</sup>

The language and placement of this provision, however, is disturbing. Although the attorney who drafted the initial version of the Act has asserted that this provision is intended to proscribe "[u]sing a computer without authority with the intent to . . . create an *improper* financial instrument,"<sup>177</sup> nothing in the computer trespass section requires fraudulent intent. The provision as written reaches any unauthorized computer use with the intent, fraudulent or otherwise, to cause any creation or alteration of a financial instrument or electronic transfer of funds.

An Arizona case, *State v. Gillies*,<sup>178</sup> illustrates conduct that the Virginia General Assembly clearly intended to proscribe with this provision. In *Gillies*, the defendant had murdered a woman and had stolen her bank card. The defendant then had used the bank card to obtain funds from the victim's bank account at an automated teller machine.<sup>179</sup> On appeal, the Arizona Supreme Court

---

173. Read in conjunction with the rest of the computer trespass section, this provision states: "Any person who uses a computer . . . without authority and with the intent to . . . [e]ffect the creation or alteration of a financial instrument or of an electronic transfer of funds . . . shall be guilty of the crime of computer trespass. . . ." VA. CODE § 18.2-152.4 (Supp. 1986).

174. See, e.g., *supra* notes 14-15 and accompanying text.

175. Letter from Daniel R. Burk, initial draftsman of the Virginia Computer Crimes Act, to Aubrey M. Davis, Jr., Commonwealth's Attorney, City of Richmond (Mar. 22, 1984) (on file at the offices of the *William and Mary Law Review*).

176. Burk, *supra* note 58, at 95; see VA. CODE § 18.2-152.2 para. 8 (Supp. 1986).

177. Burk, *supra* note 58, at 97 (emphasis added).

178. 135 Ariz. 500, 662 P.2d 1007 (1983) (en banc).

179. *Id.* at 505, 662 P.2d at 1012.

confirmed that an automated teller machine is part of a computer system, and it upheld the defendant's conviction under Arizona's comprehensive computer-assisted crime statute.<sup>180</sup>

The Virginia Computer Crimes Act, through this portion of the computer trespass section, clearly proscribes conduct such as that involved in *Gillies*, as well as any other use of a computer without authority and with the intent to effect an *improper* transfer of funds. The difficulty with the Virginia provision is that, as written, it also proscribes unauthorized computer use with the intent to effect what would be a *proper* transfer of funds. For example, suppose that an individual who possesses a bank card and needs money, but who personally cannot go to the bank, gives the card and the secret password necessary to complete the transaction to a friend, and asks that friend to use the automatic teller machine to withdraw money from the cardholder's savings account. If the friend is photographed by the camera at the ATM, as was the defendant in *Gillies*,<sup>181</sup> and later is charged with computer trespass, the unfortunate friend would have no effective defense. The friend could not claim that the ATM use was authorized because, under the terms of the usual agreement between banks and cardholders, bank cards are the property of the bank. Consequently, the hypothetical cardholder had no power to transfer the right to use the bank card to the friend. The friend also could not avoid liability by claiming that the transfer itself had been quite proper, unless the court were to read an element of fraudulent intent into the provision, because the statute as written would support a conviction merely upon evidence that the friend had received money from the ATM that had been debited to the cardholder's account. Liability would attach under the Virginia provision because, even though, unlike the defendant in *Gillies*, the friend had acted without fraudulent intent, the cardholder never had the power to authorize the friend to use the ATM; the cardholder only had the power to authorize the transfer.

One way for the General Assembly to ensure that the Act proscribes the conduct in *Gillies*, but not the conduct hypothesized above, would be to remove the offending provision from the com-

---

180. *Id.* at 506, 662 P.2d at 1013.

181. *Id.*

puter trespass section and to enact it as a separate section, but with an added element of *fraudulent* intent. This new section would read: "Any person who uses a computer without authority, and with fraudulent intent, to effect the creation or alteration of a financial instrument or of an electronic transfer of funds shall be guilty of the crime of computer trespass." The new section, in effect, would proscribe unauthorized computer use with the intent to commit the crimes of false pretenses, embezzlement, larceny by trick, and forgery, but it would not proscribe conduct not generally considered wrongful.

This legislative fix, however, would have its own problems. Consider the case of *United States v. Jones*.<sup>182</sup> In that case, Jones' brother, Everston, had entered information into his employer's accounts payable computer data file instructing the computer to substitute Jones' name for the actual payee's name on five checks totaling \$113,000. The computer dutifully had followed Everston's instructions, and had issued five checks payable to Jones. Jones subsequently had been arrested, and had been charged with transporting securities in interstate commerce knowing that they were "stolen, converted or taken by fraud."<sup>183</sup> The district court dismissed the indictment on the ground that Everston's acts constituted forgery, not false pretenses.<sup>184</sup> The United States Court of Appeals for the Fourth Circuit reversed, holding that manipulation of computer data resulting in checks payable to the computer operator's accomplice rather than to the intended payee was not forgery because "the alteration of supporting documents giving rise to the issuance of a bona fide instrument amounts to the crime of false pretenses."<sup>185</sup> The legislative fix proposed above would address Everston's conduct because Everston had "[used] a computer without authority, and with fraudulent intent, to [create] a financial instrument."<sup>186</sup> The computer fraud section of the Virginia

---

182. 553 F.2d 351 (4th Cir.), *cert. denied*, 431 U.S. 968 (1977); see also S. MANDELL, *supra* note 12, at 171 (discussing *Jones*).

183. 553 F.2d at 352 (quoting 18 U.S.C. § 2314 (1976)).

184. *Id.*

185. *Id.* at 356. The court pointed out "a valid and recognized distinction between the false making of a writing and the making of a false writing." *Id.* at 355 n.15. Everston's crime was the former, which constitutes false pretenses, not forgery.

186. See *supra* text following note 182.

Act, however, already proscribes the same conduct.<sup>187</sup> Consequently, the new section would be redundant to the extent that it proscribes false pretenses or larceny by trick.<sup>188</sup>

The new section's coverage of computer-assisted forgery, which usually occurs when an unauthorized computer user creates an invalid financial instrument that purports to be valid,<sup>189</sup> also would duplicate an existing provision in the Virginia Act. In this case, the new section would not duplicate the computer fraud section;<sup>190</sup> instead, it would duplicate a portion of the section in the Act that addresses the "[c]omputer as an instrument of forgery."<sup>191</sup> This section states: "The creation, alteration, or deletion of any computer data in any computer or computer network, which if done on a tangible document or instrument would constitute forgery under [the pre-existing forgery statute] will also be deemed to be forgery."<sup>192</sup> By providing broad-based coverage of computer-assisted forgery, this provision addresses any conduct that would be addressed in the new section proposed above, but that would not be included in the computer fraud section.<sup>193</sup> Consequently, instead of creating a new statutory section based on the fourth provision of the computer trespass section, the General Assembly should repeal this portion of the computer trespass section in favor of the computer fraud and computer as an instrument of forgery sections of the Act.

---

187. See *supra* note 119.

188. The conviction in *Gillies*, see *supra* notes 178-80 and accompanying text, also illustrates the potential redundancy. In that case, the defendant was convicted of computer fraud in the first degree under a provision in the Arizona computer-assisted crime statute, ARIZ. REV. STAT. ANN. § 13-2316(A) (Supp. 1986), that essentially prohibits the same conduct Virginia prohibits in its computer fraud provision, VA. CODE § 18.2-152.3 (Supp. 1986). See *Gillies*, 135 Ariz. at 506, 662 P.2d at 1013. This conduct also would be prohibited under the proposed new statute.

189. See R. PERKINS & R. BOYCE, *supra* note 21, at 414 ("Forgery is the fraudulent making of a false writing having apparent legal significance.").

190. See *supra* note 119.

191. VA. CODE § 18.2-152.14 (Supp. 1986). The placement of this section, at the very end of the Act, after the statute of limitations, venue, non-exclusivity, civil remedy, and severability sections, *id.* §§ 18.2-152.9 to .13, makes the provision look like an afterthought, included to make sure that the Act covered every conceivable scenario.

192. *Id.* § 18.2-152.14.

193. In fact, this provision is broader than the proposed new statute because it prohibits the use of a computer to forge *any* document of apparent legal significance, including instruments such as wills and deeds. See *id.*



*Intent to Cause Physical Injury to Another's Property*

The fifth portion of the computer trespass section prohibits unauthorized use of a computer with the intent to "cause physical injury to the property of another."<sup>194</sup> Like the proposed statutory section just discussed, this provision simply restates conduct proscribed elsewhere in the Virginia Code. For example, the intent to injure a computer falls under the second portion of the computer trespass section,<sup>195</sup> the intent to injure computer data or programs falls under the third portion of the same section,<sup>196</sup> and the intent to injure any tangible property falls under the Virginia malicious mischief statute.<sup>197</sup> Because the fifth portion of the computer trespass section adds nothing new to the law, the General Assembly should repeal it.

*Intent to Make Unauthorized Copies of Computer Data or Programs*

In 1985, the General Assembly amended the Virginia Computer Crimes Act by adding a sixth provision to computer trespass section. This provision prohibits unauthorized computer use with the intent to make "an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, [or] computer programs . . . residing in, communicated by or produced by a computer."<sup>198</sup> The new proscription greatly improved the Act, because neither other portions of the computer trespass section<sup>199</sup> nor the computer fraud section<sup>200</sup> clearly proscribes unauthorized computer use with the intent to *copy* computer data or programs. For instance, the first portion of the computer trespass section, which addresses unauthorized computer use with the intent "[t]emporarily or permanently [to] remove" information from the computer,<sup>201</sup> does not encompass this conduct because, in ob-

---

194. *Id.* § 18.2-152.4.5.

195. *See id.* § 18.2-152.4.2; *supra* notes 158-64 and accompanying text.

196. *See id.* § 18.2-152.4.3; *supra* notes 165-72 and accompanying text.

197. *See id.* § 18.2-137 (1982); *supra* note 160.

198. Act of Mar. 17, 1985, ch. 322, 1985 Va. Acts 398 (codified at VA. CODE § 18.2-152.4.6 (Supp. 1986)).

199. VA. CODE § 18.2-152.4 (Supp. 1986).

200. *Id.* § 18.2-152.3.

201. *Id.* § 18.2-152.4.1.

taining *copies* of computer programs or files, information thieves virtually never remove information from the computer.<sup>202</sup> Similarly, to the extent that the computer fraud section applies to unauthorized computer use with the intent to commit larceny or false pretenses, the computer fraud section does not proscribe this conduct, because the crimes of larceny and false pretenses also re-

---

202. An information thief can copy a program without depriving the owner of possession because of the way in which a computer operates. An operator who desires to use a particular computer program or data file first transfers the program or file from the computer's storage device into the computer's internal memory, which consists of integrated circuitry called "random access memory" (RAM). When this transfer occurs, the information contained in the program or data file does not leave the storage device; the computer simply makes a copy of the information. The operator then can view the contents of this copy by instructing the computer to display the information on the computer screen. The operator can modify, delete, or print this information by instructing the computer to perform the desired task, but modifications or deletions at this point change only the copy of the program or file located in RAM. The original program or data file in the storage device remains unchanged. When the computer operator has finished using the program or file, the operator instructs the computer to "save" any modifications or deletions. This instruction causes the computer to compare the copy of the program in RAM with the original in the storage device, and to alter the original to match the copy.

A computer operator can obtain a written copy of a program or file, without altering or removing the original, in two ways. The first method, which is the most economical, is to instruct the computer to print the entire program or file. This command tells the computer to make a "formatted" copy of the program or file, which is a copy containing special commands that tell the computer printer what to print, and to send that copy to the printer. The second method is called "screen printing," in which the operator instructs the computer to print only the information currently being displayed on the screen. That information represents a portion of the copy of the program or file in RAM. Although screen printing takes somewhat longer, a computer operator can obtain a printout of the entire program or file by displaying it piece by piece on successive screens. Because neither of these methods removes the original program or data file from the computer, the owner never is deprived of possession. Consequently, an unauthorized computer operator could obtain a written copy of a very valuable program or data file without violating the computer fraud section of the Act. The operator would commit computer fraud only by printing a copy of the particular computer program or data file and then erasing the original in the computer's storage device.

In fact, however, the "erase" command in most computers only deletes the special commands that tell the computer's operating system where to find the file in storage, and not the file itself. This feature enables a computer operator to recover the original program or file by using a special computer program designed to retrieve programs or files lacking the special locator commands. An owner of one of these computers, therefore, retains possession of a program or file even after it has been "erased," although retrieval will be difficult. In these computers, the only sure ways to erase computer programs or data files are to write another file over the area of the storage device containing the "erased" information, or to demagnetize the storage device.

quire the offender to deprive the victim of possession of the object of the crime.<sup>203</sup>

The new provision added to the computer trespass section in 1985, by applying specifically to the intent to make unauthorized copies of computerized information, closes the gap in the Act. The provision permits the Commonwealth to prosecute anyone who uses a computer without authority with the intent to copy information "residing in, communicated by or produced by a computer."<sup>204</sup> This language ensures that the provision covers all forms of computer copying, because the "residing in" language covers copies made directly from a computer's memory, the "communicated from" language covers copies made from information being transferred between remotely located computers, and the "produced by" language covers copies made of the result of calculations performed by the target computer, as well as computer printouts. The new provision also clearly states that the crime is complete the moment the user possesses the copy "in any form,"<sup>205</sup> which makes clear that an unauthorized computer user does not have to reduce the copy to paper to violate the law. Through this broad new provision, the General Assembly has given the Commonwealth a powerful tool against information thefts.

### *Computer Invasion of Privacy*

The Virginia Computer Crimes Act also prohibits "computer invasion of privacy,"<sup>206</sup> which is defined as "[intentional examination] without authority [of] any employment, salary, credit or any other financial or personal information relating to [another] per-

---

203. To the extent that the computer fraud section applies to the intent to commit the crimes of embezzlement or conversion, VA. CODE § 18.2-152.3 (Supp. 1986), the section probably does encompass unauthorized computer use with the intent to copy programs or data files. Misappropriating a copy of the true owner's property probably is a sufficient interference with the owner's rights to meet the element of "conversion" necessary to find that an embezzlement or conversion occurred, see R. PERKINS & R. BOYCE, *supra* note 21, at 358, but the determination might well depend on a factual finding as to the value of the copy to others or the decreased value of the original to the true owner, and the issue of value remains unsettled in Virginia. See *supra* notes 135-47 and accompanying text. As a result, the better charge still might be the sixth portion of the computer trespass section.

204. VA. CODE § 18.2-152.4.6 (Supp. 1986).

205. *Id.*

206. *Id.* § 18.2-152.5.

son.”<sup>207</sup> The elements of the offense are (1) use of a computer, (2) without authority, (3) intentionally to examine (4) protected information.<sup>208</sup> Because this Note already has examined the first two elements in detail,<sup>209</sup> the following discussion focuses on the final two elements.

The third element of computer invasion of privacy requires the offender intentionally to examine certain information pertaining to another person.<sup>210</sup> Under this provision, a person “examines” protected information by reviewing it after he “knows or should know that he is without authority” to review it.<sup>211</sup> This emphasis on intent and guilty knowledge limits prosecution for computer invasion of privacy to deliberate viewing of protected information. Accidental viewing does not constitute a crime.

Significantly, the crime is in the viewing itself; the offender need not manipulate the information viewed. This feature gives the Commonwealth a powerful weapon against hackers, who frequently are accused of perusing private information, especially credit records.<sup>212</sup> The Act now properly proscribes this conduct as an unwarranted invasion of privacy.

---

207. *Id.* The computer invasion of privacy section reads, in full:

A. A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. “Examination” under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

B. The crime of computer invasion of privacy shall be punishable as a Class 3 misdemeanor.

*Id.*

208. *See id.*

209. *See supra* notes 83-87 and accompanying text (“use”); *supra* notes 45-79 and accompanying text (“computer”); *supra* notes 123-27 and accompanying text (“without authority”).

210. VA. CODE § 18.2-152.5 (Supp. 1986). For purposes of the Virginia Computer Crimes Act, “person” includes not only individuals, but also any “partnership, association, corporation or joint venture.” *Id.* § 18.2-152.2 para. 10.

211. *Id.* § 18.2-152.5.

212. *See, e.g.*, 130 CONG. REC. S1179 (daily ed. Feb. 8, 1984) (remarks of Sen. Cohen) (noting instance in which hackers broke into a credit bureau computer and changed records of prominent persons).

The fourth element of computer invasion of privacy, the concept of protected information, probably evolved from the public's sensitivity to the "big brother" aspect of computers and their impact on privacy.<sup>213</sup> The General Assembly addressed this concern by outlining, in broad terms, the types of information expected to receive protection: "employment, salary, credit or any other financial or personal information relating to any other person."<sup>214</sup> This sweeping language provides expansive protection to computer owners and the subjects of their files, because it causes the statute to cover the intentional, unauthorized examination not only of computerized employment, credit, pay, and financial records, but also of the information contained in files such as medical histories and school transcripts. In fact, given the public's sensitivity to invasion of privacy by computer and the legislature's expansive response to that concern, the courts arguably should interpret this provision as encompassing any computerized information concerning a person that is not a matter of public record.

### *Theft of Computer Services*

The Act also prohibits theft of computer services. It states: "Any person who willfully uses a computer or computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services. . . ."<sup>215</sup> Because this provision explicitly requires "willful" use, it is far superior to the early federal proposals<sup>216</sup> and the state statutes based upon them.<sup>217</sup> This willfulness requirement prevents the Commonwealth from prosecuting an alleged offender for "mere" unauthorized computer use.

Commentators criticized the early federal legislative proposals because they would have punished virtually every intentional, un-

---

213. The interrelationship between computers and protection of privacy is beyond the scope of this Note. For further information, see S. MANDELL, *supra* note 12, at 171-91; D. PARKER, *supra* note 13, at 237-65.

214. VA. CODE § 18.2-152.5 (Supp. 1986).

215. *Id.* § 18.2-152.6.

216. See S. 240, 96th Cong., 1st Sess., 125 CONG. REC. 1190 (1979); S. 1766, 95th Cong., 1st Sess., 123 CONG. REC. 21,025 (1977).

217. See *supra* note 31.

authorized use of a computer,<sup>218</sup> regardless of the offender's motive. These commentators charged that the proposals were overbroad because they failed "to distinguish between felonious uses of computers, lesser criminal uses of computers, and ethically questionable or simple unauthorized uses."<sup>219</sup> They explained that programmers commonly use their employers' computers for relatively innocent activities such as playing games and drawing calendars,<sup>220</sup> writing "unauthorized" computer programs,<sup>221</sup> and performing minor personal tasks such as balancing checkbooks, charting stocks, and figuring mortgages.<sup>222</sup> Although these activities are relatively harmless, and employers' attitudes toward them vary widely,<sup>223</sup> an errant computer programmer could have been fined up to \$50,000 and sentenced to up to fifteen years in jail under the initial federal proposal.<sup>224</sup> The result, as one commentator noted, would have been "a sanction totally out of proportion to the 'offense.'"<sup>225</sup> This commentator concluded that "[e]mployment sanctions have been, and should continue to be, the adequate and proper remedy"<sup>226</sup> for such activities.

The Virginia Computer Crimes Act essentially adopts this position by requiring the offender "*willfully* [to use] the computer . . . to obtain computer services without authority."<sup>227</sup> "[W]hen used in

---

218. See S. 240, 96th Cong., 1st Sess., 125 CONG. REC. 1190 (1979) (proposed 18 U.S.C. § 1028(a)); S. 1766, 95th Cong., 1st Sess., 123 CONG. REC. 21,025 (1977) (proposed 18 U.S.C. § 1028(a)).

219. Taber, *supra* note 12, at 530.

220. *Id.*; Gemignani, *supra* note 12, at 709-10.

221. Taber, *supra* note 12, at 530.

222. *Id.*; see also Gemignani, *supra* note 12, at 710 (postulating the use of a company computer to compile bowling league statistics).

223. One commentator noted: "Some [employers] flatly forbid [computer use for personal activities]. Others forbid the practice in theory, but allow it in practice, and even 'wink' at it. Still others permit it as a fringe benefit of employment. For many companies, such use has never been considered a 'problem' that needed to be addressed." Taber, *supra* note 12, at 531 (footnotes omitted).

224. S. 1766, 95th Cong., 1st Sess., 123 CONG. REC. 21,025 (1977) (proposed 18 U.S.C. § 1028(a)). The computer-assisted crime proposal introduced in the next Congress provided for the same prison term, but changed the fine to "a sum not more than two and one-half times the amount of the fraud or theft." S. 240, 96th Cong., 1st Sess., 125 CONG. REC. 1190 (1979) (proposed 18 U.S.C. § 1028(a)).

225. Taber, *supra* note 12, at 530-31.

226. *Id.* at 531.

227. VA. CODE § 18.2-152.6 (Supp. 1986).

a criminal statute [the word "willfully"] generally means an act done with a bad purpose. . . ."<sup>228</sup> Applying this definition to the Virginia Act, the computer user not only must use the computer without authority, but also must use it with a bad purpose. If an employee uses the company computer for playing games, believing incorrectly that the employer has authorized it, that employee cannot be convicted of computer theft of services in Virginia. Even though the employee's game playing was intentional and unauthorized, the employee did not act with a bad purpose. The employee's use was not willful, and therefore it was not illegal.

Prosecutors might argue that this "willful use" requirement places a heavy burden on them because it requires proof of the accused's state of mind at the time of the unauthorized computer use. Although this argument has some merit, the "willful use" requirement should ease the prosecutors' task in the long run, because it encourages employers to promulgate useful guidelines for employee computer use so that employees accused of unauthorized computer use could not argue that their unauthorized use had been without knowledge of any illegality. Prosecutors will have little difficulty proving their cases if employers publish such guidelines and require every employee to read and abide by them.<sup>229</sup> Widespread adoption of these guidelines also would yield several other benefits: first, employers would have better control of personal computer use by employees; second, computer operators and programmers would work in an atmosphere free from uncertainty concerning personal computer use; third, employee awareness of the criminal penalties for computer theft of services likely would reduce the incidence of such theft; and fourth, the conviction rate for computer theft of services probably would be high, thus deterring others from engaging in this undesired conduct.

One problem area that would not be addressed by employee computer use guidelines would be theft of services by hackers. Although proving that a hacker who broke into another's computer obtained services "without authority" would be a simple matter because these break-ins always are without authority, proving

---

228. *United States v. Murdock*, 290 U.S. 389, 394 (1933); see also R. PERKINS & R. BOYCE, *supra* note 21, at 875-79 (discussing willfulness).

229. See Burk, *supra* note 58, at 92.

"willful" use would be another matter. Hackers often claim that they were simply "joyriding";<sup>230</sup> in other words, they claim that they were acting on a lark, and not with a bad purpose. This claim would have no force if constructive notice of this provision were sufficient to make the hacker's act "willful" but, in cases involving hackers, the Commonwealth might have to prove actual notice of the provision to meet the element of "willfulness." It might be the only way to show a bad purpose.<sup>231</sup>

The Commonwealth possibly could avoid the difficulty of proving actual notice by charging hackers with computer fraud,<sup>232</sup> on the theory that they obtained property<sup>233</sup> by false pretenses, with the fraud being the hackers' misrepresentation of their authority to use the computer.<sup>234</sup> A prosecution for computer fraud, however, should be reserved for more serious crimes. A better long-term solution would be for "educational institutions to begin teaching computer ethics along with computer competency, so that youngsters who sit down at a computer keyboard will understand the difference between a game and a crime."<sup>235</sup> The Commonwealth can apply the computer theft of services provision to hackers most effectively only when these individuals realize the consequences of their actions.

### *Personal Trespass by Computer*

The final penal section of the Act, "personal trespass by computer," prohibits unauthorized use of a computer with the intent

---

230. 130 CONG. REC. S1179 (daily ed. Feb. 8, 1984) (remarks of Sen. Cohen).

231. See *supra* note 228 and accompanying text.

232. See *supra* note 119.

233. "Property," for purposes of the Act, includes computer services. VA. CODE § 18.2-152.2 para. 11 (Supp. 1986); *supra* note 104. Although the computer fraud provision also covers unauthorized computer use with the intent to obtain "services," see *supra* note 119, the General Assembly undoubtedly meant the word "services" in that context to refer only to "traditional" services such as "labor, professional services, transportation, telephone or other public services, accommodation in motels, hotels, restaurants or elsewhere, [and] admission to exhibitions." See ALA. CODE § 13A-8-10 (1982) (listing these services in a similar provision). This construction ensures that the word "services" in the computer fraud provision has a meaning independent of the word "property." See *supra* note 134.

234. This course of action also is open to the Commonwealth with respect to any other type of computer theft of services.

235. 130 CONG. REC. E634 (daily ed. Feb. 27, 1984) (remarks of Rep. Wyden).



to cause physical injury to an individual.<sup>236</sup> Although the General Assembly labeled this crime a "trespass," courts should ignore this characterization because the language of the provision describes an assault.<sup>237</sup> The provision does not require actual injury; it requires only the *intent* to injure.

Because the Virginia Code already contains a section prohibiting simple assaults,<sup>238</sup> one could argue that the personal trespass section is redundant, and therefore unnecessary. This argument would be erroneous. Unlike the simple assault provision, which would not be applied in a prosecution for conduct that actually produced physical injury,<sup>239</sup> the personal trespass by computer section applies equally to conduct that produces injury and conduct that does not. As a result, while the usual assault becomes a felony when it produces injury, making it malicious wounding or unlawful wounding<sup>240</sup> rather than a simple assault, a personal trespass by computer becomes a felony, regardless of whether physical injury results, when the act is committed "maliciously" rather than merely "unlawfully."<sup>241</sup> This statutory scheme leads to some curious results. If an offender maliciously assaulted another individual in a face-to-face encounter, for example, the offender's crime would be the misdemeanor of simple assault, assuming that no

---

236. VA. CODE § 18.2-152.7 (Supp. 1986). The section provides, in full:

A. A person is guilty of the crime of personal trespass by computer when he uses a computer or computer network without authority and with the intent to cause physical injury to an individual.

B. If committed maliciously, the crime of personal trespass by computer shall be punishable as a Class 3 felony. If such act be done unlawfully but not maliciously, the crime of personal trespass by computer shall be punishable as a Class 1 misdemeanor.

*Id.*

237. See 2A MICHIE'S JURISPRUDENCE *Assault & Battery* §§ 2, 4 (1981).

238. VA. CODE § 18.2-57 (1982).

239. Conduct that actually produced physical injury would be malicious wounding, a Class 3 felony, or unlawful wounding, a Class 6 felony. *Id.* § 18.2-51. The Virginia Code does indicate that "assault and battery" is a lesser included offense of "malicious wounding," *id.* § 18.2-54, but the case law concerning the malicious wounding statute indicates that the lesser offense would be *simple* assault and battery, *Spradlin v. Commonwealth*, 195 Va. 523, 524, 79 S.E.2d 443, 444 (1954); *Crutchfield v. Commonwealth*, 187 Va. 291, 293, 46 S.E.2d 340, 341 (1948); *Williams v. Commonwealth*, 153 Va. 987, 992, 151 S.E. 151, 153 (1930), which is only a misdemeanor, VA. CODE § 18.2-57 (1982).

240. See VA. CODE § 18.2-51 (1982).

241. *Id.* § 18.2-152.7 (Supp. 1986).

physical injury resulted, while the same crime committed with the assistance of a computer would be a felony. Although the General Assembly may not have intended this anomalous result, the distinction remains, and provides a justification for viewing the provision as distinguishable from simple assault under other provisions of the Virginia Code.

### CONCLUSION

The revolution that has swept the computer to preeminence has carried with it a parasite—the computer-assisted crime. Computer-assisted crimes typically are just old crimes dressed in new clothes, but the law has seemed unable to cope with the unique problems these crimes present. Some computer-assisted crimes—heists involving millions—have caught the public's eye, causing law enforcement officials and legislators to react or, perhaps more accurately, to overreact to perceived inadequacies in state and federal penal codes.

The experience in Virginia illustrates well the legislative tendency to overreact to the specter of computer-assisted crime. Even though the General Assembly arguably had solved its statutory problems when it passed its first computer-assisted crime statute in 1978, it repealed that statute and replaced it with a comprehensive Act intended to “cover all the bases.” In the process, the General Assembly enacted redundant provisions and unnecessarily duplicated existing crimes.

To streamline the Act, the General Assembly should consider deleting provisions two, four, and five of the computer trespass section, and also should simplify and clarify the Act by removing every reference to “computer software” and by putting the definition of “computer program” into more understandable terms. Most importantly, the General Assembly should redefine the Act's vague definition of “computer.” The Virginia Computer Crimes Act will not become a truly effective tool for suppressing computer-assisted crime until the General Assembly modifies it to correct its significant shortcomings.

ROBIN K. KUTZ