

LEXSEE 704 A.2D 904

TERRY DEWAIN BRIGGS v. STATE OF MARYLAND

No. 24, September Term, 1997

COURT OF APPEALS OF MARYLAND

348 Md. 470; 704 A.2d 904; 1998 Md. LEXIS 9

January 22, 1998, Filed

PRIOR HISTORY: [***1]

Appeal from the Circuit Court for Anne Arundel County pursuant to certiorari to the Court of Special Appeals. Eugene M. Lerner, JUDGE.

DISPOSITION: JUDGMENT OF THE CIRCUIT COURT FOR ANNE ARUNDEL COUNTY REVERSED. COSTS TO BE PAID BY ANNE ARUNDEL COUNTY.

LexisNexis(R) Headnotes**COUNSEL:**

ARGUED BY: Bradley A. Thomas of Washington, DC, FOR APPELLANT.

ARGUED BY: Mary Ann Ince, Assistant Attorney General (J. Joseph Curran, Jr., Attorney General, on brief) of Baltimore, MD., FOR APPELLEE.

JUDGES: ARGUED BEFORE: Bell, C.J.; Eldridge, Rodowsky, Chasanow, Raker, Wilner and Karwacki (retired, specially assigned), JJ. Opinion by Raker, J.

OPINIONBY: Raker

OPINION: [*471]

[**905] Opinion by Raker, J.

Terry Dewain Briggs appeals his conviction for the crime of unauthorized access to computers, in violation of Maryland [*472] Code (1957, 1996 Repl. Vol., 1997 Supp.) Article 27, § 146(c). n1 The primary issue raised in this case is the meaning of the statutory requirement of access "without authorization" as used in § 146. The question we must answer is whether an employee who is entitled to use an employer's computer system in connection with employment duties, but who exceeds the scope of that authorization, is acting in a manner proscribed by

Article 27, § 146. Briggs contends that his conduct did not [**906] come within the prohibition of the statute. We agree, and accordingly, shall reverse.

n1 Unless otherwise specified, all statutory references herein shall be to Maryland Code (1957, 1996 Repl. Vol., 1997 Supp.) Article 27.

[***2]

I.

In November, 1994, the Scarborough Group, Inc. (Scarborough), a medium sized securities investment company, hired Terry Briggs as a computer programmer and system administrator. Briggs, a twenty-three-year old computer specialist, was hired to program and design software to maintain the company computer system. As part of his job responsibilities, he entered data in the computer system and placed passwords n2 on the files to secure the data. The management of the entire computer system was entrusted to Briggs. Following a dispute on July 24, 1995, about the terms of his employment contract, Briggs resigned as an employee of the company.

n2 A password, the most common form of user authentication, is used to prevent unauthorized access to a computer system. It is a sequence of characters that one must enter prior to gaining access to a computer. See Michael P. Dierks, *Symposium: Electronic Communications and Legal Change, Computer Network Abuse*, 6 HARV. J. L. & TECH. 307, 311 (1993).

Shortly [***3] after Briggs left the company, Scarborough realized that some of its computer files were secured with passwords known only to Briggs. Scarborough and Briggs were unable to resolve the situation. Scarborough filed a civil suit against Briggs, and also contacted the Anne Arundel County police. [*473]

The State charged Briggs in a two count criminal in-

formation: count one, theft of computers, in violation of Article 27, § 342(a)(1) n3 and, count two, unauthorized access to computers, in violation of Article 27, § 146(c)(2). At trial, Scarborough contended that Briggs changed the passwords two days before the meeting about Briggs's employment contract, and put them in a subdirectory named "ha-ha he-he," dated July 22, 1995 by the computer. Scarborough maintained that Briggs never had permission to place the company files in a directory and to protect the file with passwords, without anyone else in the company having access to the passwords. Although he denied any knowledge about "ha-ha he-he," Briggs admitted that he placed passwords on company files months earlier as part of his job in securing files, but that he had difficulty remembering the passwords because so much time had passed. Briggs [***4] suggested that Scarborough filed criminal charges against him in order to discredit him as a government witness in a Securities and Exchange Commission investigation that Briggs had initiated alleging that certain activities at Scarborough violated federal security regulations. Briggs maintained that the computer date on the password subdirectory had been changed to incriminate him.

n3 The jury acquitted Briggs of the theft charge.

The State alleged that Briggs intentionally and willfully and without authorization accessed a computer system to interrupt the operation of the computer system and computer services. In his motion for judgment of acquittal, Briggs argued that he was not guilty as a matter of law (that the statute did not apply to his activities) and as a matter of fact (that he was fulfilling his employment responsibilities). Briggs reasoned that Article 27, § 146 was not intended to apply to authorized computer users who, arguably, used their positions to cause harm to their employers by misusing [***5] the computer. The State argued that Briggs was guilty of unauthorized access, because although Briggs was authorized to access the computer system, he was not authorized to access the system in such a way as to interrupt the operation of the computer services of [*474] the system. The trial court denied Briggs's motion for judgment of acquittal, and the jury found Briggs guilty of unauthorized access to computers in violation of Article 27, § 146(c)(2)(i). The court sentenced Briggs to one year incarceration, with all but two days suspended, two years supervised probation, 150 hours of community service, and a fine of \$500. The court also ordered him to cooperate with Scarborough and required him to release any remaining password information and client files. Briggs noted a timely appeal to the Court of Special Appeals. We granted certiorari on our own motion before consideration by that court.

[**907] Appellant argues before this Court that Article 27, § 146 criminalizes the conduct of an individual who intentionally and willfully accesses a computer without authorization and is inapplicable to conduct that can be characterized as only exceeding authorized access. He concludes that the statute [***6] is inapplicable on its face because, as part of his employment, he was authorized to access the computer system. The purpose of the statute, Appellant continues, was to deter unauthorized users from *breaking into* computer systems, i.e., to prevent "hackers" n4 from gaining unauthorized access. Briggs distinguishes operating a computer system without authorization [*475] from exceeding authorized access by using the computer in an improper manner. He concludes that application of this statute to his conduct is contrary to legislative intent.

n4 The term "hacker" has been defined as "a person who views and uses computers as objects for exploration and exploitation." NATIONAL INSTITUTE OF JUSTICE, U.S. DEPT OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL xvi (2d ed. 1989) (hereinafter CRIMINAL JUSTICE RESOURCE MANUAL). A "hacker" commonly refers to a "computer user who intends to gain unauthorized access to a computer system." Michael P. Dierks, *Symposium: Electronic Communications and Legal Change, Computer Network Abuse*, 6 HARV. J. L. & TECH. 307, 310 n.7 (1993). The word "hacker" has become synonymous with a computer criminal, and typically refers to a person who breaks into computer networks. *Id.* Originally, however, the term "hacker" referred to the members of The Tech Model Railroad Club of Massachusetts Institute of Technology (TMRC) and the term "hack" referred to "a project undertaken or a product built not solely to fulfill some constructive goal, but with some wild pleasure, taken in mere involvement." *Id.* (quoting STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 23 (1984)). The terms "hack" and "hacker" found their way into the computing world when the members of TMRC began work on the digital computers at Massachusetts Institute of Technology. The TMRC resents the application of the term "hacker" to mean the committing of illegal acts, maintaining that words such as "thieves," "password crackers," or "computer vandals" are better descriptions.

[***7]

The State contends that even though access for other

348 Md. 470, *475; 704 A.2d 904, **907;
1998 Md. LEXIS 9, ***7

activities may have been authorized, a person, whether he is an employee, "hacker," or otherwise, violates the statute when that person "intentionally, willfully, and without authorization" accesses a computer system or any part of a computer system to cause the malfunction or interrupt the operations of the computer system or any part of that system. The State maintains that there was sufficient evidence to support the verdict because Briggs did not have authority to place passwords on the files without anyone else in the company having those passwords, and that he did so with the intent of interrupting the operation of the computer system.

II.

The standard for review of the denial of a motion for judgment of acquittal is "whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia*, 443 U.S. 307, 319, 99 S. Ct. 2781, 2789, 61 L. Ed. 2d 560 (1979); *see also State v. Albrecht*, 336 Md. 475, 478-79, 649 A.2d 336, 337 (1994). We do not inquire into the credibility of witnesses, [***8] or weigh the evidence to ascertain whether the State has proven their case beyond a reasonable doubt; that is the responsibility given to the trier of fact. Applying the above standard of review, we conclude that the conduct in this case does not constitute the crime of unauthorized access to computers, and the motion for acquittal should have been granted.

Article 27, § 146 provides, in pertinent part:

(c) *Illegal access.*—(1) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer [*476] system, computer services, computer data base, or any part of these systems or services.

(2) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services to:

(i) Cause the malfunction or interrupt the operation of a computer, computer network, [**908] computer software, computer control language, computer system, computer [***9] services, computer data base, or any part of these systems or services; or

(ii) Alter, damage, or destroy data or a computer program stored, maintained, or produced by a computer, computer network, computer system, computer services, computer database, or any part of these systems or services.

(3) A person may not intentionally, willfully, and without authorization:

(i) Identify or attempt to identify any valid access codes; or

(ii) Distribute or publicize any valid access codes to any unauthorized person.

Access is defined in § 146(a) as follows:

(9) "Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including, but not limited to, computers and other data processing equipment or resources connected therewith.

To support a conviction for illegal access to computers under § 146(c)(2)(i), the State must prove: (1) that Briggs intentionally and willfully accessed a computer or computer system; (2) that the access was without authorization; and (3) the access was with the intent to interrupt the operation of the computer services. We need not address Appellant's [***10] factual argument that he was authorized to place passwords on Scarborough's computer system, because we find the second element dispositive and hold that Appellant's access to the computer [*477] was not "without authorization" within the meaning of the statute. n5 When faced with a question of statutory construction, we look first to the plain meaning of the words of the statute, with the goal to ascertain and effectuate legislative intent. *Whack v. State*, 338 Md. 665, 672, 659 A.2d 1347, 1350 (1995). We give the words of the statute their ordinary and natural meaning. *Gargliano v. State*, 334 Md. 428, 435, 639 A.2d 675, 678 (1994). If the language of the statute is plain and clear and expresses a meaning consistent with the statute's apparent purpose, no further analysis is ordinarily required. *Id.* at 435, 639 A.2d at 678. On the other hand, if the language of the statute is ambiguous or unclear, "we must consider 'not only the literal or usual meaning of the words but their meaning and effect in light of the setting, the objectives and purpose of the enactment,' in our attempt to discern the construction that will best further the legislative objectives or goals." *Id.* at [***11] 436, 639 A.2d at 678 (quoting *Tucker v. Fireman's Fund Ins. Co.*, 308 Md. 69, 75, 517 A.2d 730, 732 (1986)).

n5 We recognize that "business, economic, and white-collar crimes have rapidly changed as computers proliferated into the activities and environments in which these crimes occur." NATIONAL INSTITUTE OF JUSTICE, U.S. DEPT OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL, 1 (2d ed. 1989). Scholars have noted that serious economic loss linked to computer abuse is caused by current and former employees rather than by outsiders. "In fact, the available data suggest that serious economic losses linked to computer abuse have been and continue to be attributed to current and former employees of the victimized organization rather than to interloping hackers with modems." Richard C. Hollinger and Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 116 (1988). For example, use of the employer's computer for one's own purpose may be serious, as where the employee uses the employer's computer to run his or her own business through the employer's facilities, sometimes known as "time theft." See MARTIN WASIK, CRIME AND THE COMPUTER 55 (1991). See also, NATIONAL INSTITUTE OF JUSTICE, U.S. DEPT OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL, 38-39 (2d ed. 1989). Industrial sabotage may also be inflicted by disgruntled employees. See *State v. Corcoran*, 186 Wis. 2d 616, 522 N.W.2d 226 (Wis. Ct. App. 1994).

[***12]

The statute is three-pronged. Section 146(c)(1) prohibits unauthorized access or attempted unauthorized access *per se* to computers. The actor's purpose or motive in accessing the computer—whether there is any intent to alter or damage the [*478] computer or the data on it—is irrelevant. Section 146(c)(2) prohibits unauthorized access or attempted access to computers with a further purpose, such as with the intent to cause a malfunction or interrupt the computer operation, or alter, damage, or destroy information. Section 146(c)(3) prohibits willful and intentional identification, publication, or distribution of valid access codes, and has no relevancy to the case before the Court. "Simple" unauthorized access, that is, without intent to damage or alter, is punishable by a maximum prison term of three years, a [*909] fine of \$1,000, or both. "Aggravated" unauthorized access is punishable by a maximum prison term of five years, a fine of \$5,000, or both. n6

n6 The penalty provision of Article 27, § 146

provides:

(d) *Penalty*. — (1) Any person who violates any provision of subsection (c)(1) of this section is guilty of a misdemeanor and on conviction is subject to a fine not exceeding \$1,000 or imprisonment not exceeding 3 years or both.

(2) Any person who violates any provision of subsection (c)(2) or (c)(3) of this section is guilty of a misdemeanor and on conviction is subject to a fine not exceeding \$5,000 or imprisonment not exceeding 5 years or both.

[***13]

The statute prohibits unauthorized access of a computer, computer network, or computer systems. "Access" is defined in the statute "to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including . . . computers." § 146(a)(9). "Without authorization" modifies the word "access." Therefore, the unlawful act is unauthorized access. "Authorization" is not defined in the statute. n7 Turning to dictionary definitions of "authorize," [*479] we find that BLACK'S LAW DICTIONARY 133-34 (6th Ed. 1990) defines "authorize" to mean "to empower; to give a right or authority to act. To endow with authority or effective legal power, warrant, or right. To permit a thing to be done in the future." (Citation omitted). Similarly, WEBSTER'S NEW INTERNATIONAL DICTIONARY, UNABRIDGED 186 (2d ed. 1950) defines "authorize" to mean "to clothe with authority or legal power; to give right to act; to make legal; to legalize; to give [*480] authoritative permission to or for; to justify." The testimony at trial that Briggs had authority to enter data in the computer and to place passwords on the files to secure the data establishes that he was authorized, under the statute, to "instruct, [*14] communicate with, store data in, retrieve data from and to make use of computer data [*910] equipment and other data processing equipment." The plain language of the statute suggests that if an employee were initially permitted to "instruct," "communicate with," "store data in," or "retrieve data from" the computer system, then that employee's access would be authorized. The statute makes no reference to authorized users who exceed the scope of their authority. If the Legislature intended the statute to cover employees who exceeded the scope of their authority or who misused their authority, it could have done so explicitly. n8 We conclude that the intent of the General Assembly [*481] was to criminalize the misuse of computers or computer networks by those whose initial access was unauthorized.

n7 See NATIONAL INSTITUTE OF JUSTICE, U.S. DEPT OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL xvi (2d ed. 1989), for a discussion of technical definitions in state computer crime law. The author notes that "there are now as many different and conflicting definitions of computer crime as there are states with computer crime statutes. The definitions of those terms, their comprehensibility, rate of obsolescence, and ease of application will play an important role in determining how successfully and effectively these new statutes will be used to deter and prosecute computer crime." NATIONAL INSTITUTE OF JUSTICE, U.S. DEPT OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL, 85 (2d ed. 1989).

The federal government, all of our sister states with the exception of Vermont, and most foreign countries, have responded to the problem of computer crimes. The statutes "vary widely in offense named, definitions, and sanctions." NATIONAL INSTITUTE OF JUSTICE, U.S. DEPT OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL, 83 (2d ed. 1989); see 18 U.S.C. § 1030 (1994); ALA. CODE §§ 13A-8-103 (1994 & Supp. 1996); ALASKA STAT. § 11.46.740 (1996 & Supp. 1997); ARIZ. REV. STAT. ANN. § 13-2316 (1989 & Supp. 1997); ARK. CODE ANN. §§ 5-41-101 to 107 (Michie 1997); CAL. PENAL CODE § 502 (West 1988 & Supp. 1997); COLO. REV. STAT. §§ 18-5.5-101 to 102 (1997); CONN. GEN. STAT. ANN. §§ 53a-250 to 261 (West 1994 & Supp. 1997); DEL. CODE ANN. tit. 11, §§ 931 to 939 (1995 & Supp. 1996); FLA. STAT. ANN. §§ 815.01 to .07 (West 1994 & Supp. 1997); GA. CODE ANN. §§ 16-9-91 to 94 (1996 & Supp. 1997); HAW. REV. STAT. §§ 708-890 to 893 (1994 & Supp. 1997); IDAHO CODE §§ 18-2201 to 2202 (1987 & Supp. 1997); ILL. ANN. STAT. ch. 38 para. 16D-1 to 7 (Smith-Hurd 1996); IND. CODE ANN. §§ 35-43-1-4 & 35-43-2-3 (Burns 1994 & Supp. 1997); IOWA CODE ANN. §§ 716A.1 to .16 (West 1993 & Supp. 1997); KAN. STAT. ANN. § 21-3755 (1995); KY. REV. STAT. ANN. §§ 434.840 to .860 (Michie/Bobbs-Merrill 1985 & Supp. 1997); LA. REV. STAT. ANN. §§ 14:73.1 to .5 (West 1997); ME. REV. STAT. ANN. tit. 17-A, § 357 (West Supp. 1997); MD. CODE (1957, 1996 Repl. Vol., 1997 Supp.) Article 27, § 146; MASS. GEN. L. ch. 266, § 30 (1990 & Supp. 1997); MICH. STAT. ANN. § 752.791 to .797 (Callaghan 1991

& Supp. 1997); MINN. STAT. ANN. §§ 609.87 to .891 (West 1987 & Supp. 1997); MISS. CODE ANN. §§ 97-45-1 to 13 (1994 & Supp. 1997); MO. REV. STAT. §§ 537.525, 569.093 to .099 (1988 & Supp. 1997); MONT. CODE ANN. §§ 45-2-101, 45-6-310 to 311 (1997); NEB. REV. STAT. §§ 28.1343 to .1348 (1994 & Supp. 1996); NEV. REV. STAT. ANN. §§ 205.473 to .491 (Michie 1997); N.H. REV. STAT. ANN. §§ 638:16 to :19 (1986 & Supp. 1995); N.J. STAT. ANN. §§ 2C:20-23 to 34 (1995 & Supp. 1997); N.M. STAT. ANN. §§ 30-45-1 to 7 (Michie 1989 & Supp. 1996); N.Y. PENAL LAW §§ 156.00 to .50 (McKinney 1988 & Supp. 1997); N.C. GEN. STAT. §§ 14-453 to 457 (1993 & Supp. 1996); N.D. CENT. CODE ANN. § 12.1-06.1-08 (1985 & Supp. 1997); OHIO REV. CODE ANN. §§ 2913.01, 2913.81 (Anderson 1996); OKLA. STAT. ANN. tit. 21, §§ 1951 to 1958 (West Supp. 1997); OR. REV. STAT. §§ 164.125, 164.377 (1995); 18 PA. CONS. STAT. ANN. § 3933 (1994 & Supp. 1997); R.I. GEN. LAWS §§ 11-52-1 to 8 (1994 & Supp. 1996); S.C. CODE ANN. §§ 16-16-10 to 30 (Law. Co-op. 1985 & Supp. 1996); S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to 8 (1997); TENN. CODE ANN. §§ 39-14-601 to 603 (1997); TEX. PENAL CODE ANN. §§ 33.01 to .05 (West 1989 & Supp. 1995); UTAH CODE ANN. §§ 76-6-701 to 705 (1995 & Supp. 1996); VA. CODE ANN. §§ 18.2-152.1 to .14 (Michie 1996 & Supp. 1997); WASH. REV. CODE §§ 9A.52.110 to .130 (1988 & Supp. 1996); W.VA. CODE §§ 61-3C-1 to 21 (1993 & Supp. 1997); WIS. STAT. § 943.70 (1996 & Supp. 1997); WYO. STAT. §§ 6-3-501 to 505 (1997).

[***15]

n8 The federal government and several of our sister states have explicitly prohibited computer use beyond the scope of authorization. See 18 U.S.C. § 1030(a)(1), (a)(2), (a)(4) (criminalizing access of a computer without authorization or "exceeding authorized access"). 18 U.S.C. § 1030(e)(6) defines the term "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." See also ARIZ. REV. STAT. ANN. § 13-2316(A) (Supp. 1997) (defining one element of computer fraud as accessing a computer without authorization or exceeding authorization of use); GA. CODE ANN. §§ 16-9-92 (1996 & Supp. 1997) (defining "without authority" to include the use of a computer in a manner that ex-

ceeds any permission granted by the owner of the computer); HAW. REV. STAT. §§ 708-890 (1994 & Supp. 1997) (defining "without authorization" to mean without the permission of or in excess of the permission of an owner); KAN. STAT. ANN. § 21-3755(b)(3) (1995) (defining computer crime as "intentionally exceeding the limits of authorization" in conjunction with causing damage); MICH. STAT. ANN. § 752.795 (Callaghan 1991 & Supp. 1997) (prohibiting a person from intentionally accessing a computer "without authorization or by exceeding valid authorization"); N.D. CENT. CODE ANN. § 12.1-06.1-08 (2) (Supp. 1997) (prohibiting access "in excess of authorization given or without authorization"); N.M. STAT. ANN. § 30-45-5 (Michie Supp. 1996) (criminalizing the unauthorized computer use of "any person who knowingly, willfully and without authorization, or having obtained authorization, uses the opportunity such authorization provides for purposes to which the authorization does not extend"); OHIO REV. CODE ANN. § 2913.04(B) (Anderson 1996) (prohibiting access of a computer "without the consent of, or beyond the scope of the express or implied consent of the owner"); OKLA. STAT. ANN. tit. 21, § 1953(3) (West Supp. 1997) (making it unlawful to willfully "exceed the limits of authorization" and damage, modify or alter a computer system); S.C. CODE ANN. § 16-16-20(1) (Law. Co-op. 1985 & Supp. 1996) (prohibiting the willful access to a computer "without authorization or for an unauthorized purpose").

In addition, several states have specific offenses entitled **Offenses against computer users**, which criminalize the intentional denial to an authorized user of the full and effective use of or access to a computer. *See, e.g.*, FLA. STAT. ANN. § 815.06(1) (West 1994 & Supp. 1997); LA. REV. STAT. ANN. § 73.4(A) (West 1997); MISS. CODE ANN. § 97-45-5(1)(a) (1988 & Supp. 1997); WYO. STAT. § 6-3-504 (1997).

[***16]

The legislative history supports our reading of the statute. In 1984, in an apparent response to the inadequacies of current criminal law to address disruptive or voyeuristic acts involving computer information systems, House Bill 121, approved by both houses, and enacted as Chapter 588, 1984 Laws of Maryland, criminalized "illegal access to computers." A representative of the Department of Budget and Fiscal Planning testified in support of the bill:

Generally speaking, the threat [of computer crime] may be viewed as being divided into two reasonably identifiable types: 1) those associated with criminal intent or activity, and 2) those associated with the so called "hacker" type of activity, where just the challenge of penetrating the system, or some sort of "electronic vandalism" or other mischief is the objective. While outright criminal activity involving information systems is covered by current statute, the Department feels this bill provides a needed addition by directly addressing *the second type of threat* by prohibiting all unauthorized access, for whatever purpose, and by providing penalties for its occurrence.

Testimony Regarding House Bill 121, Department [***17] of Budget and Fiscal Planning (available at the Department of Legislative Reference, Bill File for House Bill 121 (1984)) (emphasis [*482] added). The legislative history thus suggests that House Bill 121 was drafted in reaction to the concern about the recent "hacker" activity. The Senate Judicial Proceedings Committee Report for House Bill 121, reported favorably by Chairman (now President of the Senate) Thomas [*911] V. Mike Miller, underscores our conclusion that the statute should apply to those who break into computers:

BACKGROUND:

Proponents of this bill testified that, under current law, simply breaking into a computer system to vandalize or cause other mischief is not illegal. Thus, the bill was introduced by those who feel unauthorized access alone should be a misdemeanor subject to penalties.

LEGISLATIVE INTENT:

This legislation is intended to make it a misdemeanor for a person intentionally and without authorization to access, attempt to access or cause access to a computer system. *The purpose of the bill is to deter individuals from breaking into computer systems.*

Committee Report System, Summary of Committee [***18] Report, House Bill 121 (available at the Department of Legislative Reference, Bill File for House Bill 121 (1984)) (emphasis added). The 1989 amendment to the statute, House Bill 1065, enacted as Chapter 722, 1989 Laws of Maryland, added subsections (c)(2) and (3)

thereby creating two new substantive crimes with more severe penalties. Subsection (c)(2) prohibits a person from intentionally and willfully accessing a computer to cause malfunction or interrupt the operation of a computer, or to alter, damage or destroy data or program stored by a computer, and subsection (c)(3) prohibits a person from intentionally, willfully, and without authorization attempting to identify or distribute computer passwords. n9 The Senate Judicial [*483] Proceedings Committee Bill Analysis and Floor Report concerning House Bill 1065 states:

n9 In addition to creating two new substantive crimes, House Bill 1065 expanded the scope of computer access activities punishable as crimes by changing the definitions such that "computer database" included data produced by a computer or computer system, or a computer network. The bill also extended the definition of "computer network" to include computers intermittently connected. Article 27, § 146(a)(1), (4).

***19]

BACKGROUND:

This bill upgrades current computer access provisions to address recent well publicized disruptions of public and private computer systems, and invasions of personal privacy by "hackers."

* * * * *

The first new crime penalizes the damage which hackers may wreak in illegally accessed systems, above and beyond the current penalty for the access itself.

Id. (available at the Department of Legislative Reference, Bill File for House Bill 1065 (1989)). Once again, it appears that the General Assembly sought to address the perceived threat from "hackers," and, in particular, the damages that they may cause beyond mere browsing. *See also* Testimony Regarding House Bill 1065, Delegate Samuel Rosenberg (stating "much of the current crisis revolves around underground 'hackers'") (available at the Department of Legislative Reference, Bill File for House Bill 1065 (1989)). Contrary to the State's argument, the legislative history thus suggests that House Bill 1065 was designed to enlarge the *penalties* related to mischievous unauthorized access, not to enlarge the definition of access. These comments and reports suggest [***20] that the intent of the Legislature was to punish access that was not initially authorized and not to punish conduct that merely exceeded authorized access.

Briggs's access was not unauthorized under Article 27, § 146, the unauthorized access to computers statute. If the law is to be broadened to include Briggs's conduct, it should be modified by the Legislature, not by this Court. [*484]

JUDGMENT OF THE CIRCUIT COURT FOR ANNE ARUNDEL COUNTY REVERSED. COSTS TO BE PAID BY ANNE ARUNDEL COUNTY.