University of Baltimore Law Forum

Volume 28
Number 2 *Summer 1998*

Article 5

1998

Recent Developments: Briggs v. State: Conviction for Unauthorized Access to Computers Cannot Stand Where Defendant Misused Employer's Computers, but Was Authorized to Use Them in Connection with Employment Duties

William H. Jones

Briggs v. State:

CONVICTION FOR UNAUTHORIZED ACCESS TO COMPUTERS CANNOT STAND WHERE DEFENDANT MISUSED EMPLOYER'S COMPUTERS, BUT WAS AUTHORIZED TO USE THEM IN CONNECTION WITH EMPLOYMENT DUTIES

By William H. Jones

Interpreting Maryland's statute prohibiting unauthorized access to computers, the Court of Appeals of Maryland, in *Briggs v. State,* 348 Md. 470, 704 A.2d 904 (1998), held that a defendant's conviction under that statute cannot stand where the defendant was actually authorized to use his employer's computers. The decisions suggests that it is left to the General Assembly to determine if such conduct should be criminalized.

Terry Briggs ("Briggs") began working for the Scarborough Group, Inc. ("Scarborough") as a computer specialist in November, 1994. He was responsible for the management of the entire computer system, with duties that included data entry and the placing of passwords on computer files. Briggs resigned from his position with Scarborough in July, 1995, following a dispute over the terms of his contract.

Soon thereafter, Scarborough discovered that it could not access some computer files because Briggs was the only person who knew the passwords. Unable to settle the dispute with Briggs, Scarborough sued Briggs and reported the situation to the Anne Arundel County Police Department. Briggs was charged under Article 27, §§ 342, 146(c)(2) of the Annotated Code with theft of computers and unauthorized access to computers. (1996 & Supp. 1997).

The crux of the State's argument was that Briggs changed the passwords, something he was not entitled to do unless someone else in the company was given the changed passwords. Briggs claimed that he could not remember the passwords due to the length of time which had elapsed since placing them on the files in dispute. In a motion for judgment of acquittal, Briggs argued that section 146 did not apply to his conduct, claiming that the statute was not intended to punish authorized users who misuse their employer's computers. The trial court denied Briggs's motion and the jury convicted him of unauthorized access to computers. Briggs filed an appeal and on its own motion, the court of appeals granted certiorari.

The court first noted that for Briggs to be convicted under article 27, section 146 (c)(2)(I), the State must prove: "1) that Briggs intentionally and wilfully accessed a computer or computer system; 2) that the access was without authorization; and 3) that the access was with the intent to interrupt the operation of the computer services." *Briggs,* 348 Md. at 476, 704 A.2d at 908. The court then focused on the second element of the offense, lack of authorization, which it determined to be dispositive. *Id.* at 476-77, 704 A.2d at 908.

The court first looked to the plain meaning of the statute at issue in order to ascertain legislative intent. *Id.* At 476-77, 704 A.2d at 908, (citing *Whack v. State*, 338 Md. 665, 672, 659 A.2d 1347, 1350 (1995)). Noting that the word "authorization" was not defined in the statute, the court consulted dictionaries for a generally accepted definition of "authorize." The court found phrases such as "to empower," "to permit a thing to be done," "to give a right or authority to act," and "to clothe with authority or legal power." *Briggs*, 348 Md. at 479-80, 704 A.2d at 909.

With these definitions of "authorize," the court concluded the plain meaning of the statute was to prohibit persons without authorization from accessing computer systems. *Id.* at 480-81, 704 A.2d at 910. The statute did not speak of persons who go beyond the scope of authority granted to them, or misuse such authority. *Id.* The court noted that the evidence at Briggs's trial established that he was authorized to use the computer system to enter data and place passwords on files. *Id.* at 480, 704 A.2d at 909-10. As such, he possessed the authority that must in fact be absent to support his conviction. *Id.* at 480-81, 704 A.2d at 910.

The court of appeals also analyzed the legislative history of the statute. *Id.* at 481, 704 A.2d at 910. In 1984, House Bill 121 was introduced to the Legislature as a measure to criminalize "'illegal access to computers.'" *Id.* The

court examined testimony in support of the bill and found that its purpose was to deter "hacker" activity, where the goal is to penetrate the computer system. *Id.* at 482, 704 A.2d at 910. Specifically, it was discovered that in the Senate Judicial Proceedings Committee Report for House Bill 121, the legislature sought to "deter individuals from breaking into computer systems.'" *Id.*, 704 A.2d at 911. An amendment to the statute added two subsections that created two new substantive crimes. *Id.* Here, the legislative intent behind the amendment appeared to be the imposition of criminal liability on "hackers" for the damage they cause to computer systems after gaining access without authorization. *Id.* at 483, 704 A.2d at 911. Again, the Legislature appeared to be concerned with "hackers" who never had authorization to use the computer systems.

Based on its interpretation of Maryland's unauthorized access to computers statute, supported by plain meaning analysis and an examination of legislative history, the Court of Appeals of Maryland reversed Briggs's conviction, holding that a person can not be convicted under the statute when authority has been granted to that person to use the computer system. However, the argument can be made that if one reads the statute plainly, focusing on the words that apply to the facts in *Briggs,* the statute actually reads that a person may not intentionally, willfully, and without authorization access a computer system to cause the malfunction, or interrupt the operation of a computer network. With this reading of the statute, one could argue that Briggs did violate the statute, as although he had authorization to access the computer system, he did not have authorization to do so to interrupt the operation of the system. In *Briggs v. State,* the court of appeals made clear that to criminalize acts done to a computer system by a person authorized to access the system, the Legislature must act to include users who exceed their authority.