STATE OF KANSAS
v.
ANTHONY A. ALLEN

No. 74,639

SUPREME COURT OF KANSAS

260 Kan. 107 (1996)

LARSON, J.: In this first impression case, we are presented with the question of whether a person's telephonic connections that prompt a computer owner to change its security systems constitute felony computer crime in violation of *K.S.A. 21-3755(b)*.

The charges against Anthony A. Allen arose from several telephonic connections he made with Southwestern Bell Telephone Company's computers in early 1995. After preliminary hearing, the trial court dismissed the complaint, finding no probable cause existed to believe Allen had committed any crime.

The State has appealed pursuant to *K.S.A. 22-3602(b)(1)*. We affirm the trial court.

Because the result in this case must be limited to and driven by the facts presented at the preliminary hearing, we will summarize the evidence there presented in considerable detail.

Allen admitted to Detective Kent Willnauer that he had used his computer, equipped with a modem, to call various Southwestern Bell computer modems. The telephone numbers for the modems were obtained by random dialing. If one of Allen's calls were completed, his computer determined if it had been answered by voice or another computer. These were curiosity calls of short duration.

The State presented no evidence which showed that Allen ever had entered any Southwestern Bell computer system. Detective Willnauer was unable to state that Allen had altered any programs, added anything to the system, used it to perform any functions, or interfered with its operation. Willnauer specifically stated he had no evidence that the Southwestern Bell computer system had been damaged.

Ronald W. Knisley, Southwestern Bell's Regional Security Director, testified Allen had called two different types of Southwestern Bell computer equipment--SLC-96 system environmental controls and SMS-800 database systems.

The telephone numbers for the SLC-96 systems were thought to be known only to Southwestern Bell employees or agents on a need-to-know basis. Access to the SLC-96 systems required knowledge of a password. If one connected to **[***5]** the system it displayed "KEYWORD?" without any identification or warning. No evidence existed that Allen attempted to respond to the prompt.

Testimony confirmed Allen also called and connected 28 times with the SMS-800 systems at several different modem numbers. Each call but two was under 1 minute. Upon connection with this system, a person would see a log on request and a "banner." The banner identifies the system that has answered the incoming call and displays that it is Southwestern Bell property and that access is restricted. Entry into the system itself then requires both a user ID and a password which must agree with each other. No evidence indicated Allen went beyond this banner or even attempted to enter a user ID or password.

Knisley testified that if entry into an SMS-800 system were accomplished and proper commands were given, a PBX system could be located which would allow unlimited and nonchargeable long distance telephone calls. There was no evidence this occurred, nor was it shown that Allen had damaged, modified, destroyed, or copied any data.

James E. Robinson, Function Manager responsible for computer security, testified one call to an SMS-800 system lasted 6 minutes and 35 seconds. Although the system should have retained information about this call, it did not, leading to speculation the record-keeping system had been overridden. Robinson speculated Allen had gained entry into the system but admitted he had no evidence that Allen's computer had done anything more than sit idle for a few minutes after calling a Southwestern Bell modem number.

Robinson testified that Southwestern Bell was unable to document any damage to its computer equipment or software as a result of Allen's activities. However, as a result of its investigation, Southwestern Bell decided that prudence required it to upgrade its password security system to a more secure "token card" process. It was the cost of this investigation and upgrade that the State alleges comprises the damage caused by Allen's actions. Total investigative costs were estimated at $ 4,140. The cost of developing deterrents was estimated to be $ 1,656. The cost to distribute secure ID cards to employees totalled $ 18,000. Thus, the total estimated damage was $ 23,796.

In closing arguments, the State admitted Allen did not get into the computer system, nor did he modify, alter, destroy, copy, disclose, or take possession of anything. See *K.S.A. 21-3755(b)(1)*. Instead, the State argued Allen's conduct in acquiring the unlisted numbers and calling them constituted an "approach" to the systems, within the meaning of *K.S.A. 21-3755(a)(1)*, which questioned the integrity of the systems and resulted in the altered or added security precautions. . . .

The legal standard to be applied in a preliminary hearing is clear. If it appears from the evidence presented that a crime has been committed and there is probable cause to believe the defendant committed it, *K.S.A. 22-2902(3)* requires that the defendant be bound over for trial. *State v. Martinez, 255 Kan. 464, 466, 874 P.2d 617 (1994)*. If there is not sufficient evidence, the defendant must be discharged. *State v. Engle, 237 Kan. 349, 350, 699 P.2d 47 (1985)*; *K.S.A. 22-2902(3)*. From the evidence presented, the trial court must draw the inferences favorable to the prosecution, and the evidence need only establish probable cause. *State v. Sherry, 233 Kan. 920, 935, 667 P.2d 367 (1983)*. "Probable cause at a preliminary hearing signifies evidence sufficient to cause a person of ordinary prudence and caution to conscientiously entertain a reasonable belief of the accused's guilt." *State v. Puckett, 240 Kan. 393, Syl. P 1,729 P.2d 458 (1986)*.

Allen was charged under *K.S.A. 21-3755*, which in applicable part provides:

"(a) As used in this section, the following words and phrases shall have the meanings respectively ascribed thereto:

"(1) '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.

"(2) 'Computer' means an electronic device which performs work using programmed instruction and which has one or more of the capabilities of storage, logic, arithmetic or communication and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network."

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

....

"(6) 'Computer system' means a set of related computer equipment or devices and computer software which may be connected or unconnected.

....

"(8) 'Property' includes, but is not limited to, financial instruments, information, electronically produced or stored data, supporting documentation and computer software in either machine or human readable form.

....

"(b) Computer crime is:

"(1) Intentionally and without authorization gaining or attempting to gain access to and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property;

....

"(c) ...

"(2) Computer crime which causes a loss of the value of at least $ 500 but less than $ 25,000 is a severity level 9, nonperson felony.

....

"(e) Criminal computer access is intentionally, fraudulently and without authorization gaining or attempting to gain access to any computer, computer system, computer network or to any computer software, program, documentation, data or property contained in any computer, computer system or computer network. Criminal computer access is a class A nonperson misdemeanor."

Allen was charged with a violation of *K.S.A. 21-3755(b)(1)*, with the second amended complaint alleging that he

> "did then and there intentionally and without authorization gain access and damage a computer, computer system, computer network or other computer property which caused a loss of the value of at least $ 500.00 but less than $ 25,000.00, a severity level 9 non-person felony."

Felony computer crime as it is charged in this case under *K.S.A. 21-3755(b)(1)* required the State to prove three distinct elements: (1) intentional and unauthorized access to a computer, computer system, computer network, or any other property (as property is defined in *K.S.A. 21-3755[a][8]*); (2) damage to a computer, computer system, computer network, or any other property; and (3) a loss in value as a result of such crime of at least $ 500 but less than $ 25,000. The trial court found that the State failed to show probable cause as to each of these elements.

Did the trial court err in ruling there was insufficient evidence to show Allen gained "access" to Southwestern Bell's computers?

After finding the evidence showed Allen had done nothing more than use his computer to call unlisted telephone numbers, the trial court ruled there was insufficient evidence to show Allen had gained access to the computer systems. Although a telephone connection had been established, the evidence showed Allen had done nothing more. The trial court reasoned that unless and until Allen produced a password that permitted him to interact with the data in the computer system, he had not "gained access" as the complaint required.

The State argues the trial court's construction of the statute ignores the fact that "access" is defined in the statute, *K.S.A. 21-3755(a)(1)*, as "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." By this definition, the State would lead us to believe that any kind of an "approach" is criminal behavior sufficient to satisfy a charge that Allen did in fact "gain access" to a computer system.

The problem with the State's analysis is that *K.S.A. 21-3755(b)(1)* does not criminalize "accessing" (and, thus, "approaching") but rather "gaining or attempting to gain access." If we were to read "access" in this context as the equivalent of "approach," the statute would criminalize the behavior of "attempting to gain approach" to a computer or computer system. This phrase is lacking in any common meaning such that an ordinary person would have great difficulty discerning what conduct was prohibited, leading to an effective argument that the statute was void for vagueness. See *State v. Adams, 254 Kan. 436, Syl. P 1, 866 P.2d 1017 (1994)*.

The United States Department of Justice has commented about the use of "approach" in a definition of "access" in this context: "The use of the word 'approach' in the definition of 'access,' if taken literally, could mean that any unauthorized physical proximity to a computer could con-

stitute a crime." National Institute of Justice, Computer Crime: Criminal Justice Resource Manual, p. 84 (2d ed. 1989).

We read certain conduct as outside a statute's scope rather than as proscribed by the statute if including it within the statute would render the statute unconstitutionally vague. See *Flax v. Kansas Turnpike Authority, 226 Kan. 1, 9, 596 P.2d 446 (1979)*. Consequently, although *K.S.A. 21-3755* defines "access," the plain and ordinary meaning should apply rather than a tortured translation of the definition that is provided. See *State Dept. of SRS v. Public Employee Relations Board, 249 Kan. 163, 168, 815 P.2d 66 (1991)* (statutory words presumed used in ordinary and common meanings).

In addition, *K.S.A. 21-3755* is certainly rendered ambiguous by the inclusion of the definition of "access" as a verb when its only use in the statute is as a noun. As a criminal statute, any ambiguity is to be resolved in favor of the accused. See *State v. JC Sports Bar, Inc., 253 Kan. 815, 818, 861 P.2d 1334 (1993)* (criminal statutes construed strictly against the State).

Webster's defines "access" as "freedom or ability to obtain or make use of." Webster's New Collegiate Dictionary, p. 7 (1977). This is similar to the construction used by the trial court to find that no evidence showed that Allen had gained access to Southwestern Bell's computers. Until Allen proceeded beyond the initial banner and entered appropriate passwords, he could not be said to have had the ability to make use of Southwestern Bell's computers or obtain anything. Therefore, he cannot be said to have gained access to Southwestern Bell's computer systems as gaining access is commonly understood. The trial court did not err in determining the State had failed to present evidence showing probable cause that Allen had gained access to Southwestern Bell's computer system.

Did the trial court err in ruling that no evidence showed Allen had damaged any computer, computer system, computer network, or any other property?

The State acknowledges it cannot meet the damage element of the crime it has charged by any means other than evidence showing Allen's actions resulted in expenditures of money by Southwestern Bell. It is crystal clear there is absolutely no evidence Allen modified, altered, destroyed, copied, disclosed, or took possession of anything. The State's evidence clearly shows Allen did not physically affect any piece of computer equipment or software by his telephone calls. All the State **[***15]** was able to show was that Southwestern Bell made an independent business judgment to upgrade its security at a cost of $ 23,796. The State argues this is sufficient.

The State's argument is clearly flawed. The trial court reasoned by a fitting analogy that the State is essentially saying that a person looking at a no trespassing sign on a gate causes damage to the owner of the gate if the owner decides as a result to add a new lock. The trial court has clearly pointed to the correct analysis of this issue.

The State's circular theory is that if someone incurs costs to investigate whether an activity is criminal, it becomes criminal because investigative costs were incurred. Although computer crime is not, for obvious reasons, a common-law crime, it nevertheless has a common-law predicate which helps us to understand the legislature's intent. *K.S.A. 21-3755* was not designed to

update criminal trespass or malicious mischief statutes to the computer age but "to address inadequacies in the present theft statute related to prosecution of computer related crimes. Specifically, present theft statutes make prosecution difficult among crimes in which the computer owner was not actually deprived of the computer or its software." Kansas Legislature Summary of Legislation 1985, p. 80.

Theft, as defined in *K.S.A. 21-3701*, is not concerned with mere occupation, detention, observation, or tampering, but rather requires permanent deprivation. The intent required for theft is an "intent to deprive the owner permanently of the possession, use, or benefit of the owner's property." *K.S.A. 21-3701(a)*. One may have wrongful intent, such as intent to trespass, without having the intent required for a theft. Perkins and Boyce, Criminal Law, p. 326 (3d ed. 1982). In addition, at common law, the thing of which the victim was deprived had to be something of value. Perkins & Boyce, Criminal Law, p. 296. The second element of computer crime mirrors this common-law requirement of the deprivation of something of value in a larceny action. As in a larceny action, the extent of the deprivation determines the severity level of the crime. This element of computer crime, as with other theft statutes, cannot be satisfied where there is no deprivation as in this case.

The State argues that investigative costs qualify as damages under the statute because investigative costs may be recovered from the perpetrator of computer crime as restitution. See *State v. Lindsly, 106 Ore. App. 459, 808 P.2d 727 (1991)*. In our case, the issue is whether Allen's conduct is rendered criminal because it was investigated, not whether restitution for conduct already determined to be criminal includes investigative costs. *Lindsly* has no application to the present case.

The degree of a theft crime is established by the value of the stolen property. See *State v. Wilson & Wentworth, 221 Kan. 359, 363, 559 P.2d 374 (1977)*. Restitution, in contrast, can include not only the fair market value of the property lost, but other costs in connection with the theft as well. See *State v. Hinckley, 13 Kan. App. 2d 417, 419, 777 P.2d 857 (1989)*. The amount of restitution can be greater than the damages used to classify the crime. It requires only a causal connection between the crime proved and the loss on which restitution is based. *State v. Wells, 18 Kan. App. 2d 735, 737, 861 P.2d 828 (1993)*. We will not utilize the State's "restitution" theory to determine if there is probable cause to determine that the damage elements of a crime have been shown.

Southwestern Bell's computer system was not "damaged" in the sense the statute requires. Southwestern Bell was not deprived of property in the manner required to support a criminal charge. The fact an independent business judgment that Southwestern Bell's computer systems might be accessible was made after Allen's conduct was discovered does not support the second and third elements of the crime charged. The trial court correctly determined the State failed to meet its probable cause burden on these issues as well.

Affirmed.