STATE OF MICHIGAN

COURT OF APPEALS

PEOPLE OF THE STATE OF MICHIGAN, Plaintiff-Appellant,	UNPUBLISHED September 10, 1999
v	No. 217190 Macomb Circuit Court
HENDRIK B. HELLEMAN, Defendant-Appellee.	LC No. 98-002619 FH

Before: Hoekstra, P.J., and O'Connell and R.J. Danhof,* JJ.

PER CURIAM.

The prosecution appeals by right from the circuit court's order granting defendant's motion to quash the information and dismiss the charge of intentional and unauthorized access of a computer for the purpose of acquiring, altering, damaging, deleting, or destroying property or other use, with a resulting loss of an aggregate amount of $20,000 or more, MCL 752.795; MSA 28.529(5); MCL 752.797(1)(d)(i); MCL 28.529(7)(1)(d)(i), against defendant. We affirm.

Defendant was a technical expert performing computer simulated crash testing for Breed Technologies, Inc. (Breed), a multinational supplier of steering wheels, seat belts, air bags, and electronic sensors to the automobile industry. Prior to his termination, defendant was engaged in a computer simulation project evaluating two different seat belts. This project, known as the HP-1 program, entailed processing data generated by Breed through a computer simulation program known as MADYMO. The project was concluded in February 1998, and defendant's report indicated no performance improvements. In March 1998, defendant was terminated, but was allowed to spend several unsupervised hours at his work station. Shortly thereafter, Breed's customer on the HP-1 project desired to look at the raw data, but an examination of the hard drive on the Silicon Graphics Indigo computer (one of only three or four such computers at Breed) previously used by defendant, revealed that the hard drive had been purged of data files, and that only the operating systems and the MADYMO program were present. Defendant was contacted, and he indicated that a backup tape was among the tapes left at this office. Breed personnel attempted to read the tape on their equipment, but could not do so. A backup tape previously archived with a data storage company was retrieved by

* Former Court of Appeals judge, sitting on the Court of Appeals by assignment.

Breed, but it too could not be read by Breed's equipment. Finally, defendant provided a third backup tape that he apparently had in his possession, in contravention of his nondisclosure agreement with Breed. This tape also could not be read. After criminal charges were filed against defendant, he took one of the backup tapes to Silicon Graphics, where the tape was read and transferred to a medium readable by Breed's equipment. The district court bound defendant over on the instant charge, but the circuit court granted a defense motion to quash, finding that the information was always within the dominion of its owner, and that Breed did not suffer an aggregate loss of $20,000 or more.

We review the legal issue of whether alleged conduct falls within the scope of a particular statute de novo. *People v Thomas*, 438 Mich 448, 452; 475 NW2d 288 (1991). However, the factual sufficiency with regard to a district court's decision to bind a defendant over on a charge is reviewed for an abuse of discretion. *People v Ozarme*, 224 Mich App 551, 557; 570 NW2d 118 (1997). Because these are the same standards employed by the circuit court upon review of the district court's determination, this Court's review of the circuit court's decision may be said to be de novo. *Id.* The underlying question is whether there was probable cause to believe that a felony had been committed and that defendant committed it. MCL 766.13; MSA 28.931; MCR 6.110.

"Probable cause that the defendant has committed the crime charged is established by a reasonable ground of suspicion, supported by circumstances sufficiently strong in themselves to warrant a cautious person in the belief that the accused is guilty of the offense charged." *People v Tower*, 215 Mich App 318, 321; 544 NW2d 752 (1996). Here, defendant was charged with causing an aggregate loss to Breed of over $20,000 by intentionally, and without authorization, deleting the raw data for the HP-1 project from the hard drive of his SGI computer. As it applies to this case, the charged offense comprises three elements: (1) intentional and unauthorized access to a computer, (2) for the purpose of acquiring, damaging, deleting, or destroying property, (3) resulting in a loss of an aggregate amount of $20,000 or more. MCL 752.795(a); MSA 28.529(5)(a); MCL 752.797(1)(d)(i); MSA 28.529(7)(1)(d)(i). See CJI2d 30.15. We conclude that the prosecution failed to demonstrate probable cause as to any of these elements.

As to the first and second elements, no evidence was presented that defendant intentionally and without authorization accessed the computer information for any illegal purpose. Apparently in recognition of the difficulty in proving intent under the act, the Legislature amended the statute, pursuant to 1996 PA 326, to add subsection 7(3), which provides:

> (3) It is a rebuttable presumption that the person did not have authorization from the owner, system operator, or other person who has authority from the owner or system operator to grant permission to access the computer program, computer, computer system, or computer network or has exceeded authorization unless 1 or more of the following circumstances existed at the time of access:
>
> (a) Written or oral permission was granted by the owner, system operator, or other person who has authority from the owner or system operator to grant permission of the accessed computer program, computer, computer system, or computer network.

(b) The accessed computer program, computer, computer system, or computer network had a pre-programmed access procedure that would display a bulletin, command, or other message before access was achieved that a reasonable person would believe identified the computer program, computer, computer system, or computer network as within the public domain.

(c) Access was achieved without the use of a set of instructions, code, or computer program that bypasses, defrauds, or otherwise circumvents the pre-programmed access procedure for the computer program, computer, computer system, or computer network. [MCL 752.797(3); MSA 28.529(7)(3).]

Here, the prosecution failed to establish a presumption of unauthorized access in accordance with subsection 7(3), given the evidence that, at all times prior to his leaving Breed's employ on March 6, 1998, defendant had permission to access his computer. We note, in particular, that prosecution witness Haran testified that defendant was fired on March 6, 1998, at about 3:00 p.m., but allowed to return to his cubicle without escort or restriction. The prosecution presented no evidence that defendant in fact accessed the computer at his desk after he was fired, or that, assuming he did, the access was unauthorized. Moreover, another Breed employee, who also used a Silicon Graphics computer, testified that after a project was completed he normally deleted the relevant data files from his hard drive after storing that data on tape. No evidence was presented that defendant knew there would be a problem reading the backup copies. Apparently, neither Breed nor the prosecution attempted to have one of the backup tapes read by more sophisticated equipment at Silicon Graphics, the vendor of the computer at issue. While it was defendant, after he had been charged with a crime, who took a backup tape to Silicon Graphics to have it read, as far as the record indicates, Breed could have performed this same task at any time with one of the several backup tapes it had in its possession.

As a general rule, a criminal defendant's intent may be inferred from the facts and circumstances of a case. *People v Phillips*, 385 Mich 30, 37; 187 NW2d 211 (1971). However, "'[w]here a defendant's acts are of themselves commonplace or equivocal, and are as consistent with innocent activity as they are with criminal, it will be necessary for the government to adduce objective facts to establish criminal intent.'" *People v Jory*, 443 Mich 403, 419; 505 NW2d 228 (1993), quoting *Seeney v United States*, 563 A2d 1081, 1083-1084 (DC App, 1989). Here, the prosecution has failed to adduce any objective evidence of criminal intent or illegal purpose by defendant. Thus, probable cause as to the first and second elements was not established.

As to the third element, we conclude that the prosecution failed to present evidence that any illegal act allegedly committed by defendant resulted in a loss of an aggregate amount of $20,000 or more, as required by MCL 752.797(1)(d)(i); MCL 28.529(7)(1)(d)(i). The act includes the following definition:

(2) 'Aggregate amount' means any direct or indirect loss incurred by a victim including, but not limited to, the value of any money, property or service lost, stolen, or rendered unrecoverable by the offense, or any actual expenditure incurred by the victim to verify that a computer program, computer, computer system, or computer network

was not altered, acquired, damaged, deleted, disrupted, or destroyed by the access. [MCL 752.792(2); MSA 28.529(2)(2).]

The prosecution presented no evidence at the preliminary examination that Breed suffered a direct or indirect loss in an "aggregate amount" of $20,000 as a result of either data that was "lost, stolen, or rendered unrecoverable by the offense," or "any actual expenditure incurred . . . to verify that a computer program . . . was not altered, acquired, damaged, deleted, disrupted, or destroyed by the access." The only evidence presented with respect to the amount of loss incurred by Breed was Mr. Cooper's testimony that it would cost the company approximately $150,000 to regenerate the lost data. However, the prosecution conceded to the circuit court that Breed was in possession of the data and that it was not required to expend any money to regenerate it. Thus, the prosecution failed to establish probable cause as to the third element.

Given the foregoing, we hold that the prosecution did not establish probable cause as to any of the elements of the charged offense, and that, as a consequence, the circuit court was correct in granting defendant's motion to quash the information.

Affirmed.

/s/ Joel P. Hoekstra
/s/ Robert J. Danhof