COURT OF APPEALS OF VIRGINIA

Present: Judges Benton, Bumgardner and Frank
Argued at Richmond, Virginia

SUSIE M. PLASTERS

v. Record No. 1870-99-3

COMMONWEALTH OF VIRGINIA

MEMORANDUM OPINION* BY
JUDGE RUDOLPH BUMGARDNER, III
JUNE 27, 2000

FROM THE CIRCUIT COURT OF ALLEGHANY COUNTY
Duncan M. Byrd, Jr., Judge

Terry N. Grimes (King, Fulghum, Snead, Nixon & Grimes, P.C., on brief), for appellant.

Shelly R. James, Assistant Attorney General (Mark L. Earley, Attorney General, on brief), for appellee.

The trial court convicted Susie M. Plasters of five counts of computer invasion of privacy in violation of Code § 18.2-152.5. She contends the evidence was insufficient to support her convictions. One count charged that she committed computer invasion of privacy against Catherine Humphries on July 16, 1998 by accessing personal information about her from a computer terminal in West Virginia. The Commonwealth concedes the evidence was insufficient to prove the defendant accessed a computer terminal in West Virginia. Accordingly, we reverse

* Pursuant to Code § 17.1-413, recodifying Code § 17-116.010, this opinion is not designated for publication.

that conviction, but we conclude the evidence is sufficient to support the other four convictions.

When the sufficiency of the evidence is challenged on appeal, we view the evidence and all reasonable inferences fairly deducible therefrom in the light most favorable to the Commonwealth. See Commonwealth v. Presley, 256 Va. 465, 466, 507 S.E.2d 72, 72 (1998). The statement of facts established that the defendant worked as a part-time dispatcher for the Covington Police Department from February 1995 through January 1999. She was trained and certified to use the Virginia Criminal Information Network (VCIN) in February 1995 and again in October 1997 when she received the highest possible grade. As a dispatcher, the defendant could obtain confidential personal information only by entering her individual user-identification number which her employer had provided. Each time the network was accessed, the following notice appeared on the computer screen: "Information obtained from VCIN may be used for criminal justice purposes only."

The defendant worked as a dispatcher on each of the dates specified in the indictments. Her unique identification number was used to access restricted information from VCIN using a computer terminal at the Covington Police Department. To obtain personal information about a particular person, the operator had to enter either the name or social security number of that person. The defendant concedes she "understood that dispatchers

could not use the VCIN computer to access criminal histories of persons without prior authorization or pursuant to a formal request."

"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." Code § 18.2-152.5(A). The evidence must establish the offender viewed the information after she knew or should have known she was unauthorized to do so. See id.

The defendant concedes she accessed the information alleged, but contends she did not know she was unauthorized to do so because it was personal, not criminal history, information. This argument is without merit for two reasons.

First, the defendant knew she was unauthorized to access criminal information from the VCIN computer without proper authorization. The records she accessed on the four dates alleged in the indictment contain criminal history information. On May 10, 1998, the information she obtained on Barry Dean Abshire included "Previous DWI: 01 10." On October 2, 1998, the defendant retrieved information on Clayton Wayne Gaylor which included "Previous DWI: 01 06" and "driver license status - suspend[ed]/habitu[al]." On October 24, 1998, the defendant also received information that Gaylor was a "wanted person" for "failure to appear" for a DUI charge. On April 10, 1998, she

obtained information on Terri Lynn Carper that included "Previous DWI: 00." This information, which the defendant concedes she accessed, clearly constitutes criminal history information. As to the invasion of Carper's privacy, we find that even though she did not have a DWI record, that data is still criminal history information.

Additionally, the VCIN warning indicates that any "information obtained from VCIN may be used for criminal justice purposes only." VCIN's restriction on the use of its data is not limited to criminal history information. Thus, even if the defendant accessed personal information alone, her use, unless properly authorized or requested, would be unlawful.

Finally, it does not matter that the defendant did not know accessing personal information was a crime. The training the defendant received did not specifically address Code § 18.2-152.5, but "ignorance of the law is no excuse." See Miller v. Commonwealth, 25 Va. App. 727, 731-32, 492 S.E.2d 482, 485 (1997) ("Although leading at times to seemingly 'unfair' results, rigid application of the rule promotes the policy it serves: 'to encourage people to learn and know the law.'" (citations omitted)). See Shea v. Virginia State Bar, 236 Va. 442, 444, 374 S.E.2d 63, 64 (1988) (all attorneys are responsible for knowing disciplinary rules).

The defendant was using the VCIN computer to access data without authorization and without any request for the

information. Each time the defendant accessed VCIN, the terminal displayed the warning that use of any information was limited to criminal justice purposes only. Her duties as a dispatcher provide no separate reason to need or use the data. She was not using the computer for any criminal justice purpose.

We conclude the evidence is sufficient to prove beyond a reasonable doubt that the defendant intentionally used the VCIN terminal to examine criminal history and other personal information of other persons after she knew or should have known she lacked any authority to do so. Accordingly, we affirm the convictions other than the one for which the Commonwealth confessed error.

Affirmed in part,
reversed in part.

Benton, JR., dissenting.

I concur in reversing the conviction for computer invasion of privacy concerning Catherine Humphries. I dissent, however, from the holding that the evidence was sufficient to prove Susie Plasters committed the other computer invasion of privacy offenses.

Plasters was convicted of violating the following statute:

> 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.

Code § 18.2-152.5(A). The Commonwealth failed to prove Plasters "review[ed] the information . . . after the time at which [she knew] or should [have known] that [she was] without authority to view the information displayed." Id.

The statement of facts established that Plasters and other dispatchers for the Covington Police Department received certification training. Plasters had last taken this training in 1997; however, the course did not cover the prohibitions contained in Code § 18.2-152.5. The training course instructor "testified that course materials prepared for instruction given

in 1999 did address Code § 18.2-152.5, and had Plasters' employment not been terminated in January 1999, Plasters would have received training at the 1999 certification session addressing Code § 18.2-152.5, among other things." Indeed, the outline for the 1999 recertification course specifically notes that the training will include "Personal Trespass by Computer under Code of Virginia 18.2-152.7," which is a topic that was not included in the course's previous outline.

Plasters testified "that she understood that dispatchers could not use the VCIN computer to access criminal histories of persons without prior authorization or pursuant to a formal request." (Emphasis added.) She knew this because the employee handbook contained the following information directed toward dispatchers:

> Article 134. Criminal History Records:
>
> Dispatchers shall not release or show any criminal history record to any individual, organization or company without the expressed permission of the Chief of Police.
>
> Under no circumstances shall any criminal history information obtained through VCIN or NCIC be released to other than legally constituted Criminal Justice agencies. Local criminal history records are not to be released except to the above-described agencies.
>
> The improper release of criminal history information could result in the termination of VCIN and NCIC services.

> All messages seeking criminal history records shall be recorded in the terminal log. (Emphasis added.)

None of the fifteen articles in the handbook relating to the job duties of dispatchers contain an admonition against viewing personal or non-criminal history information.

Kenneth R. Lane, an officer with the Department, testified for the Commonwealth that the information Plasters accessed "did not include information concerning criminal histories, employment, salary, credit or other financial information." Clearly, if the Commonwealth's own expert witness testified that Plasters did not access "criminal histories," Plasters could not be expected to know the information would contain what the majority opinion now asserts to be "information . . . [that] constitutes criminal history." The evidence is undisputed that Plasters did not access the Central Criminal Records Exchange maintained by the State Police. Furthermore, no evidence in the record establishes that Plasters knew that she was not authorized to access Department of Motor Vehicles and non-criminal history information on the VCIN computer. Code § 18.2-152.5 by its specific terms requires proof that Plasters knew or should have known that she had no authority to review the personal information she accessed on the computer.

I disagree with the suggestion that in this case we must give rigid application to the rule that "ignorance of the law is

no excuse." Miller v. Commonwealth, 25 Va. App. at 731, 492 S.E.2d at 485. As we noted in Miller, where we did not rigidly apply that rule, "[t]he rationale underlying the rule is less compelling for crimes that are malum prohibitum, viz., acts that are 'wrong because prohibited,' not by virtue of their inherent character." Id. at 731-32, 492 S.E.2d at 485 (citation omitted). Indeed, Code § 18.2-152.5 specifically bars rigid application of that rule to this offense. The statutory language itself reflects the General Assembly's policy decision that each person's level of knowledge must be considered in applying this criminal statute.

Moreover, I do not believe it is reasonable to expect the police department's lay employee to know that State law differs from what she is taught in her "official training." It is clear from the record that the Department's training course had not covered this aspect of the Code of Virginia as it relates to Plasters' job. Furthermore, nothing in the record establishes that Plasters was required as a part of her employment to go beyond her training and independently read the Code.

Thus, proof that Plasters knew she was not authorized to "use the VCIN computer to access criminal histories" was not sufficient to support this conviction where the evidence proved only that she viewed personal information that was not a criminal history. Although the VCIN system displayed a warning that "information obtained from VCIN may be used for criminal

justice purposes only," that warning did not state that viewing the information was prohibited and it did not define "used." "When a word is not defined . . . we normally construe it in accord with its ordinary or natural meaning." Smith v. United States, 508 U.S. 223, 228 (1993). In discussing the definition of the term "use," the United States Supreme Court has said the following:

> Webster's defines "to use" as "[t]o convert to one's service" or "to employ." Webster's New International Dictionary of English Language 2806 (2d ed. 1949). Black's Law Dictionary contains a similar definition: "[t]o make use of; to convert to one's service; to employ; to avail oneself of; to utilize; to carry out a purpose or action by means of." Black's Law Dictionary 1541 (6th ed. 1990). Indeed, over 100 years ago we gave the word "use" the same gloss, indicating that it means "'to employ'" or "'to derive service from.'" Astor v. Merritt, 111 U.S. 202, 213 (1884).

Smith, 508 U.S. at 228-229. Although Plasters admitted that she viewed the information after she accessed it on her computer, no evidence in the record proved that Plasters "used" the information for any purpose.

Under the terms of the statute, it does matter whether Plasters knew she was without authority to view personal information. The Commonwealth is required to prove beyond a reasonable doubt that she "reviewed the information . . . after the time at which [she knew] or should [have known] that [she was] without authority to view the information displayed." Code

§ 18.2-152.5(A). Thus, it is significant and fatal to these convictions that Plasters did not know she was without authority to view personal information.

For these reasons, I would reverse all the convictions. Therefore, I dissent.