COURT OF APPEALS OF VIRGINIA

PUBLISHED

Present: Chief Judge Huff, Judges Decker and AtLee
Argued at Chesapeake, Virginia

CRYSTAL GAIL RAMSEY

v. Record No. 0123-15-1

COMMONWEALTH OF VIRGINIA

OPINION BY
CHIEF JUDGE GLEN A. HUFF
DECEMBER 29, 2015

FROM THE CIRCUIT COURT OF THE CITY OF NORFOLK
Everett A. Martin, Jr., Judge

Adam M. Carroll (Wolcott Rivers Gates, on briefs), for appellant.

John W. Blanton, Assistant Attorney General (Mark R. Herring, Attorney General, on brief), for appellee.

Crystal Gail Ramsey ("appellant") appeals her thirteen misdemeanor convictions of computer invasion of privacy, in violation of Code § 18.2-152.5. Following a bench trial in the Circuit Court of the City of Norfolk ("trial court"), appellant was sentenced to 210 days in the Norfolk City jail, with 180 days suspended. On appeal, appellant contends that "[t]he trial court erred in finding sufficient evidence, specifically that [appellant] intentionally examined identifying information of another person without authority through the use of a computer network, in violation of [Code] § 18.2-152.5." For the following reasons, this Court affirms appellant's convictions.

## I. BACKGROUND

On appeal, "we consider the evidence and all reasonable inferences flowing from that evidence in the light most favorable to the Commonwealth, the prevailing party at trial." Williams v. Commonwealth, 49 Va. App. 439, 442, 642 S.E.2d 295, 296 (2007) (*en banc*)

(quoting Jackson v. Commonwealth, 267 Va. 666, 672, 594 S.E.2d 595, 598 (2004)). So viewed, the evidence is as follows.

Between August 1, 2012 and April 1, 2013, appellant, a state trooper with the Virginia Department of State Police, ran inquiries on fifteen individuals[1] using the Virginia Criminal Information Network ("VCIN"). Some individuals, such as appellant's girlfriend, Sara Jensen ("Jensen"), specifically asked appellant to run inquiries on their criminal history or personal information through VCIN. Several other inquiries that were run on other individuals were run on appellant's own initiation. Appellant admitted to the investigating officer, Master Trooper Eric Bruno ("Bruno"), that the inquiries were not run for any criminal justice purpose.

In her position as a state trooper, appellant had been granted access to VCIN, which allowed her to access DMV information, "wanted person" information, and driving records. To access someone's criminal history, appellant had to make inquiries through a dispatcher who, after appellant gave the purpose for her request, would then forward her the information. The dispatcher would not verify the validity of the request but would assume the request was made for a proper purpose. Such was the case for one victim, Michael Evans ("Evans"), who was Jensen's supervisor at the time appellant made inquiry into his criminal history. To obtain criminal history information on Evans, appellant requested dispatch to forward her Evans's criminal history for use in a "firearms case," even though Evans had neither owned a firearm nor applied or otherwise sought to acquire one. Appellant had never met Evans and had not opened an investigation file on him.

Dispatcher Senior Tina Wilson ("Wilson") testified that she trained appellant on the use of VCIN. Wilson confirmed that each time a VCIN inquiry is made, the user will see a message

[1] Each of these inquiries served as the basis for a separate charge. The trial court dismissed two of these charges because one individual was deceased and there was insufficient evidence of the existence of another individual.

that states "information obtained from VCIN may be used for criminal justice purposes only." Additionally, on the VCIN recertification test, which appellant took, question 7 states: "True/False: DMV information obtained through VCIN can only be used for criminal justice purposes." Wilson testified further that she instructs everyone she trains that not even a person with the highest level of access is permitted to use VCIN to run inquiries on themselves or another person for non-criminal justice purposes. Bruno also confirmed that "[s]tate troopers are only to use VCIN for law enforcement purposes, not to learn things about their neighbors," or other non-criminal justice purposes.

For running these inquiries without a criminal justice purpose, appellant was charged with violating Code § 18.2-152.5. During trial, appellant moved to strike on the ground that the evidence was insufficient to show she did not have authority to access the information. Specifically, appellant argued that no manual defining the scope of authority had been submitted into evidence and that the VCIN warning and recertification test only restrict the *use* of information obtained from VCIN.

Following a bench trial, the trial court found appellant guilty of thirteen counts of misdemeanor computer invasion of privacy. Specifically, the trial court concluded that appellant "had no authority to examine [the] identifying information" of the thirteen individuals she ran inquiries on and, therefore, was in violation of Code § 18.2-152.5. This appeal followed.

## II. STANDARD OF REVIEW

When considering on appeal the sufficiency of the evidence presented below, we "presume the judgment of the trial court to be correct" and reverse only if the trial court's decision is "plainly wrong or without evidence to support it." Davis v. Commonwealth, 39 Va. App. 96, 99, 570 S.E.2d 875, 876-77 (2002) (citations omitted). We do not "substitute our judgment for that of the trier of fact." Wactor v. Commonwealth, 38 Va. App. 375, 380, 564

S.E.2d 160, 162 (2002). Rather, "the relevant question 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 (1979). In doing so, this Court "gives full play to the responsibility of the trier of fact fairly to resolve conflicts in the testimony, to weigh the evidence, and to draw reasonable inferences from basic facts to ultimate facts." Id. In addition, any matters of statutory interpretation are reviewed *de novo* on appeal. Scott v. Commonwealth, 58 Va. App. 35, 48, 707 S.E.2d 17, 24 (2011).

## III. ANALYSIS

On appeal, appellant contends that the trial court erred in ruling that the evidence was sufficient to find that she was without authority to use VCIN to examine the personal and criminal history information of others. Appellant argues that she had the authority to access VCIN for any purpose and that the only evidence of any limitation to this authority was the VCIN warning and the question on the recertification test, which only restricted her *use* of the information obtained from VCIN.

Under Code § 18.2-152.5(A),

> [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 identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3, relating to any other person.

(Emphasis added). For the purposes of Code § 18.2-152.5(A), an offender acts "'without authority' when he knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission." Code § 18.2-152.2. "Examination" is further defined as reviewing the identifying information of

another "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). In summary, to be convicted under this section the evidence must establish that the offender viewed identifying information of another "when he knows or reasonably should know" he is without right, agreement, or permission to do so or "act[ing] in a manner knowingly exceeding such right, agreement, or permission." Code §§ 18.2-152.2, 18.2-152.5; see also Plasters v. Commonwealth, No. 1870-99-3, 2000 Va. App. LEXIS 473, at *3 (Va. Ct. App. June 27, 2000) ("The evidence must establish the offender viewed the information after she knew or should have known she was unauthorized to do so.").

The only Virginia appellate case concerning violations of Code § 18.2-152.5 is the unpublished decision in Plasters, 2000 Va. App. LEXIS 473. In Plasters, this Court upheld the appellant's conviction, concluding that the evidence was sufficient to find that the appellant, a police dispatcher, knew she only had authority to access VCIN for criminal justice purposes. Id. at *3. Significantly, this Court found that it is the unauthorized use of a computer or computer network to access data that constitutes a violation of Code § 18.2-152.5, without regard to whether the information is subsequently used. Id. at *5-6. In deciding that the appellant "knew or should have known" that she had exceeded the scope of her authority, this Court found the evidence was sufficient considering she knew she could not access criminal history information, which was included in some of the inquiries she made, and considering the warning statement that displayed every time she accessed VCIN. Id. at *4-5. This Court reasoned that the appellant lacked the authority to view the information on VCIN for non-criminal justice reasons given that "[h]er duties as dispatcher provided no separate reason to need or use the data" obtained and the warning that appeared each time she used VCIN stated "*any* 'information obtained from VCIN

may be used for criminal justice purposes only.'" Id. at *5-6. We find the reasoning of Plasters to be persuasive.

The same year the General Assembly adopted Code § 18.2-152.2, Congress enacted similar legislation, *viz.*, the Computer Fraud and Abuse Act. 18 U.S.C. § 1030; see LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009). In pertinent part, the federal act is similar to Virginia's proscription. The federal act makes it a crime to obtain information by computer "without authorization or exceed[ing] authorized access." 18 U.S.C. § 1030(a)(2), (e)(6). In United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010), the Eleventh Circuit affirmed the conviction of an employee of the Social Security Administration who accessed the personal records of seventeen individuals using the Administration's databases "for nonbusiness reasons." Id. at 1260. In his defense, the employee claimed that he did not violate 18 U.S.C. § 1030 because he only accessed the information through databases "he was authorized to use" as an employee of the Administration. Id. at 1263. The court rejected the employee's argument as "ignor[ing] both the law and the record." Id. The court found that evidence of the mandatory training sessions, posted notices, and a daily computer screen banner notice established that the Administration's policy was to permit use of its databases "only when done for business reasons." Id. at 1260, 1263. The employee's access of personal information for any reason unrelated to his duties as an employee of the Administration was, therefore, in violation of the plain language of the act. Id. at 1263. This ruling was not altered by the employee's argument that he was accessing the information as part of a "whistle-blowing operation" and that "he did not use the information to further another crime or to gain financially." Id. at 1260, 1262. Affirming the employee's conviction, the court explained "the misdemeanor penalty provision of the Act . . . does not contain any language regarding purposes for committing the offense." Id. at 1264. Therefore, the "use of information is irrelevant if [the employee] *obtained the information*

*without authorization* or as a result of exceeding authorized access." Id. at 1264 (emphasis added). "[The employee] exceeded his authorized access and the Act does not require proof that [he] used the information to further another crime or to gain financially." Id. at 1260.

Code § 18.2-152.5 similarly provides that "the crime of computer invasion of privacy [is committed] when [a person] uses a computer or computer network and *intentionally examines without authority* any . . . information . . . relating to any other person." (Emphasis added). The use to which the information may be put is not relevant. Appellant argues that the only evidence of any limitation on her authority was the warning on the VCIN network and the question on her recertification test but this argument ignores the testimony of both Wilson and Bruno who confirmed that troopers are instructed during training that they are only to use VCIN for law enforcement purposes. Appellant concedes that her "authority" to access VCIN stems from her employment as a state trooper and to maintain this access she had to be re-certified. Wilson testified that during such re-certification appellant was informed that one is not even permitted to run his own information or that of family members through the system. Furthermore, the language in the recertification test and the warning message from the network itself served as a reminder of the department's policy that VCIN was to be used for "criminal justice purposes" only. Moreover, appellant understood this "criminal justice purpose" limitation on her authority to access VCIN as evidenced by her use of a fictitious "firearms investigation" to gain access to the criminal history of Evans. Therefore, the evidence is sufficient to find appellant was without authority to examine the information on VCIN for non-criminal justice purposes.

## IV. CONCLUSION

For the foregoing reasons, this Court affirms the ruling of the trial court and finds the evidence was sufficient to find appellant was acting "without authority" when she used VCIN for non-criminal justice purposes, in violation of Code § 18.2-152.5.

Affirmed.