COURT OF APPEALS OF VIRGINIA

PUBLISHED

Present: Judges Petty, Beales and Chafin
Argued at Richmond, Virginia

MARVIN T. RIDEOUT, III

v. Record No. 0513-13-2

COMMONWEALTH OF VIRGINIA

OPINION BY
JUDGE RANDOLPH A. BEALES
FEBRUARY 4, 2014

FROM THE CIRCUIT COURT OF NEW KENT COUNTY
Thomas B. Hoover, Judge

J. Todd DuVal (McDonald, Sutton & DuVal, PLC, on brief), for appellant.

John W. Blanton, Assistant Attorney General (Kenneth T. Cuccinelli, II, Attorney General, on brief), for appellee.

Pursuant to a conditional guilty plea agreement, Marvin T. Rideout, III (appellant) entered pleas under North Carolina v. Alford, 400 U.S. 25 (1970) ("Alford pleas") to twenty counts of possession of child pornography in violation of Code § 18.2-374.1:1(A).[1] Appellant argues that the trial court erred in denying his motion to suppress evidence supporting these convictions because appellant claims that the police breached his reasonable expectation of privacy in the contents of his personal computer – files from which appellant had displayed to the public through peer-to-peer, file-sharing software. We hold that the trial court did not err when it denied appellant's motion to suppress, and, accordingly, for the following reasons, we affirm appellant's twenty convictions for possession of child pornography.

[1] Appellant had been charged with twenty additional counts of possession of child pornography, one count of distribution of child pornography, and two counts of distribution of child pornography (second or subsequent violation). As part of the conditional plea agreement, the Commonwealth disposed of those remaining charges by *nolle prosequi*.

I. BACKGROUND

We consider the evidence on appeal "'in the light most favorable to the Commonwealth as we must since it was the prevailing party'" in the trial court. Beasley v. Commonwealth, 60 Va. App. 381, 391, 728 S.E.2d 499, 504 (2012) (quoting Riner v. Commonwealth, 268 Va. 296, 330, 601 S.E.2d 555, 574 (2004)). In this case, Sergeant Stephen Anders of the Bedford County Sheriff's Office (assigned to the Southern Virginia Internet Crimes Against Children Task Force) conducted an authorized, remote undercover investigation into the online sexual exploitation of children on the internet. On August 29, 2011, a certain internet protocol (IP) address of 174.66.3.142 caught his attention. Sergeant Anders suspected that this IP address was involved in the collection and sharing of child pornography. On September 1, 2011, through a program called "Shareaza LE,"[2] Sergeant Anders was able to connect to, and begin downloading, a known file of child pornography from IP address of 174.66.3.142. On September 2, 2011, and on September 4, 2011, Sergeant Anders again was able to connect to the IP address of 174.66.3.142 and begin to download child pornography files.

Sergeant Anders also obtained and submitted an administrative subpoena to Cox Communications, the owner of the IP address at issue. In response to that administrative subpoena, Cox Communications informed Sergeant Anders that the IP address had been issued to Marvin Rideout of New Kent, Virginia.

On December 15, 2011, after verifying that "Marvin Rideout" was, in fact, the suspect detected by Special Agent Anders, Detective J. McLaughlin, III, of the New Kent County

[2] Shareaza is a peer-to-peer sharing program that allows users to trade electronic files, including music, photographic, and video files. Shareaza LE is the law enforcement version of Shareaza which, according to Sergeant Anders, differs from the regular Shareaza in that it does not permit law enforcement to share files with other users.

Sheriff's Office, obtained a search warrant for appellant's residence.[3] Detective McLaughlin executed the search warrant at appellant's residence on the following morning. When Detective McLaughlin explained to appellant why he was there, appellant put his head down and said, "I have been waiting for y'all to come." Sergeant Anders then analyzed various electronic items seized from appellant's home, finding many images and movies depicting child pornography.

Appellant filed a pre-trial motion to suppress the three files of child pornography giving rise to the search warrant (i.e., the files that Sergeant Anders was able to access on September 1, 2, and 4 of 2011), as well as all of the files found as a result of execution of the search warrant. At the suppression hearing, appellant testified that he had downloaded a software program called "Shareaza" somewhere between two and three years prior to the suppression hearing. Shareaza is, according to appellant's expert Eric Myer, designed to facilitate the sharing of files – "it wants to share." As Sergeant Anders also explained, with respect to peer-to-peer sharing programs like Shareaza, "the whole purpose is for everybody to share." Appellant had previously used a peer-to-peer file sharing program called Limewire for several years prior to downloading Shareaza, so he had several years of experience with peer-to-peer software. Appellant explained that, when he initially downloaded the Shareaza software, he had applied settings that he thought would prevent others from being able to access files on his computer. According to the theory advanced by appellant at the suppression hearing, despite selecting settings on Shareaza to

[3] Sergeant Anders prepared an affidavit in support of the application for a search warrant in which he provided the issuing magistrate with an extensive description of peer-to-peer (P2P) software and how computer files are shared and accessed using that software. Sergeant Anders explained, "When the P2P software is installed on a computer, the user is directed to specify a 'shared' folder. All files placed in that user's 'shared' folder are available to anyone on the world-wide network for download." Sergeant Anders also indicated that the law enforcement version of Shareaza "uses only publicly available P2P options which follow the programming language (protocols) set forth in the public P2P protocol standards." Accordingly, Sergeant Anders stated in the affidavit, "No functionality outside of the publicly available protocols is added, thus eliminating any potential private intrusion on the suspect IP's computer or files."

prevent sharing, however, when appellant changed the location of the downloads from the default destination, he inadvertently activated the sharing of that folder without receiving any notification that he was actually sharing files.[4] Thus, appellant claimed at the suppression hearing that he had been using the Shareaza software under the mistaken impression that he had set up Shareaza in a way that would prevent other users from gaining access to any files on his computer.

At the time of the suppression hearing, appellant's counsel and the Commonwealth stipulated to certain facts, including: (1) that any efforts appellant made to block access to his computer were ineffective when Sergeant Anders was able to obtain the three child pornography files from appellant's computer, and (2) that law enforcement "did not 'hack' or otherwise use nefarious means" to gain access to appellant's computer, but did so only through a modified version of Shareaza (that was designed to prevent the police from sharing child pornography with others). Appellant argued that he nonetheless had a reasonable expectation of privacy relating to the contents of his personal computer, including the files depicting child pornography, because he contended that he had applied settings to Shareaza that he thought would prevent others from accessing those files on his own computer. In overruling appellant's motion to suppress, the trial court stated as follows:

> The Court makes the following findings: . . . The Court finds that the defendant had no reasonable expectation of privacy when he installed a software program on his computer which has the primary purpose to share information among other computer users. Number two, that the police did not act in an improper manner to obtain information from the defendant's computer. And therefore the motion to suppress is denied.

[4] Sergeant Anders testified that it was also possible to add folders into the library through a "sharing manager" window. That window indicates clearly that any folders added to it will be shared.

Appellant thereafter entered Alford pleas to twenty charges of possessing child pornography, and reserved the right to appeal the trial court's ruling on appellant's motion to suppress.

II. ANALYSIS

In reviewing a trial court's denial of a motion to suppress, "[t]he burden is on the defendant to show that the denial of his suppression motion, when the evidence is considered in the light most favorable to the Commonwealth, was reversible error." McCain v. Commonwealth, 261 Va. 483, 490, 545 S.E.2d 541, 545 (2001) (citing Fore v. Commonwealth, 220 Va. 1007, 1010, 265 S.E.2d 729, 731 (1980); Weathers v. Commonwealth, 32 Va. App. 652, 658, 529 S.E.2d 847, 850 (2000)). On appeal, we review "*de novo* the trial court's application of defined legal standards such as whether a defendant had a reasonable expectation of privacy sufficient to permit him to raise a Fourth Amendment challenge to a search." Sharpe v. Commonwealth, 44 Va. App. 448, 454, 605 S.E.2d 346, 349 (2004) (citing United States v. Gordon, 168 F.3d 1222, 1225 (10th Cir. 1999)). Furthermore, we are "bound by the trial court's findings of historical fact unless 'plainly wrong' or without evidence to support them and we give due weight to the inferences drawn from those facts by resident judges and local law enforcement officers." McGee v. Commonwealth, 25 Va. App. 193, 198, 487 S.E.2d 259, 261 (1997) (en banc) (quoting Onelas v. United States, 517 U.S. 690, 699 (1996)).

A. WHETHER APPELLANT ESTABLISHED AN EXPECTATION OF PRIVACY

The Fourth Amendment of the United States Constitution states,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue, but upon probable cause, supported by oath of affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

"Since Katz v. United States, 389 U.S. 347 (1967), the touchstone of [Fourth] Amendment analysis has been the question whether a person has a 'constitutionally protected reasonable

expectation of privacy.'" Oliver v. United States, 466 U.S. 170, 177 (1984) (quoting Katz, 389 U.S. at 360 (Harlan, J., concurring)). Thus,

> in order to claim the protection of the Fourth Amendment, a defendant must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable; i.e., one that has "a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."

Minnesota v. Carter, 525 U.S. 83, 88 (1998) (quoting Rakas v. Illinois, 439 U.S. 128, 143-44 n.12 (1978)); see also Smith v. Maryland, 442 U.S. 735, 740-41 (1979) (adopting Justice Harlan's two-prong reasonable expectation of privacy test from his concurrence in Katz, 389 U.S. 347, which first looks at the person's subjective expectation of privacy and then considers whether that view is objectively reasonable).[5] Appellant contends that, given his claim that he disabled the sharing features of Shareaza, he then retained a reasonable expectation of privacy in the contents of his computer and in the files located on his computer that could otherwise be shared via Shareaza.

In Smith, 442 U.S. at 740, the United States Supreme Court explained:

> Consistently with Katz, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a "justifiable," a "reasonable," or a "legitimate expectation of privacy" that has been invaded by government action. [(Citations omitted).] This inquiry, as Mr. Justice Harlan aptly noted in his Katz concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy," 389 U.S., at 361 -- whether, in the words

[5] While recent United States Supreme Court decisions such as United States v. Jones, 132 S. Ct. 945 (2012), have considered Fourth Amendment principles from the perspective of whether a trespass to property has occurred, the Supreme Court has stated that the Katz reasonable expectation of privacy test has been added to this Fourth Amendment trespass test. According to the Supreme Court, "Situations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis." Jones, 132 S. Ct. at 953. Thus, it is appropriate to apply the Katz test here.

> of the Katz majority, the individual has shown that "he seeks to preserve [something] as private." Id., at 351. The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable,'" id. at 361-- whether, in the words of the Katz majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances. Id. at 353. [(Foonote and citations omitted).]

Thus, an individual can claim Fourth Amendment protection under this test only if (1) the individual has a subjective expectation of privacy *and* (2) the individual has an objectively reasonable expectation of privacy that is justifiable under the circumstances.

Even though appellant testified that he was under the impression that he had disabled the sharing feature on Shareaza, the record establishes that appellant actually said to Detective McLaughlin, "I have been waiting for y'all to come." Viewing the evidence in the light most favorable to the Commonwealth, as we must since it prevailed below, this statement in itself strongly suggests that appellant knew or at least suspected that files from his computer were able to be shared. Indeed, a rational trier of fact assessing the testimony at the suppression hearing could infer from this statement that appellant was aware that he was not the only individual with access to those files due to his installation of the Shareaza program. Certainly, the trial court was not obligated to believe appellant's self-serving testimony that he believed that he had safeguarded his files containing child pornography from being shared on Shareaza – which, of course, is peer-to-peer software actually *designed for the sharing* of files over the internet. See Marable v. Commonwealth, 27 Va. App. 505, 509-10, 500 S.E.2d 233, 235 (1998).

Here, the trial court expressly found that appellant lacked a reasonable expectation of privacy "when he installed a software program on his computer which has the primary purpose to share information among other computer users." We, like the trial court, find several federal appellate court decisions to be applicable and instructive on this point. "'Although as a general matter an individual has an objectively reasonable expectation of privacy in his personal

computer, we fail to see how this expectation can survive [appellant's] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program.'" United States. v. Stults, 575 F.3d 834, 843 (8th Cir. 2009) (quoting United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008)). Thus, by simply installing file-sharing software onto his computer, appellant has "'failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable.'" Id. Appellant's installation of Shareaza presents a situation that is analogous to a person who hands over the keys to his house to a number of friends. That person should not be surprised when some of those friends simply come inside his house without knocking on the door. Id.

Appellant contends, however, that his claimed attempt to apply settings to Shareaza to prevent others from accessing his files depicting child pornography creates an objectively reasonable expectation of privacy in those computer files. However, the decision in United States v. Borowy, 595 F.3d 1045, 1047 (9th Cir. 2010), is highly persuasive on the facts here. In Borowy, the defendant claimed that he had attempted to engage the feature in his version of peer-to-peer file-sharing software that would prevent others from downloading and viewing his files. However, that feature was not actually engaged, and an FBI agent was able to access incriminating files from the defendant's computer. Id. Concluding that the defendant's "subjective intention not to share his files did not create an objectively reasonable expectation of privacy in the face of such widespread public access," id. at 1048, the appellate court affirmed the lower court's decision to deny the defendant's motion to suppress. Id. at 1049.

Applying the logic in Borowy to this case, therefore, even assuming without deciding that appellant actually had the subjective intention to prevent others from accessing his files, appellant still did *not* have an objectively reasonable expectation of privacy in those files, given his decision to install the Shareaza file-sharing program on his computer. Indeed, appellant

installed software on his computer that is specifically designed to share files from one's own computer with other users of that software. By installing the Shareaza peer-to-peer file sharing software on his computer, appellant assumed the risk that other users of Shareaza – including the police – could readily access those incriminating files that could be shared through Shareaza.

B. THE EXCLUSIONARY RULE

During oral argument before this Court, appellant's counsel argued that suppression of the evidence would still be appropriate because it was a police officer who accessed the child pornography files shared from appellant's computer. However, this case is not one where the suppression of evidence would even serve any of the rationales underlying the purpose of the exclusionary rule. The United States Supreme Court has explained:

> First, the exclusionary rule is not an individual right and applies only where it "'result[s] in appreciable deterrence.'" We have repeatedly rejected the argument that exclusion is a necessary consequence of a Fourth Amendment violation. Instead we have focused on the efficacy of the rule in deterring Fourth Amendment violations in the future.
>
> In addition, the benefits of deterrence must outweigh the costs. "We have never suggested that the exclusionary rule must apply in every circumstance in which it might provide marginal deterrence." "[T]o the extent that application of the exclusionary rule could provide some incremental deterrent, that possible benefit must be weighed against [its] substantial social costs." The principal cost of applying the rule is, of course, letting guilty and possibly dangerous defendants go free—something that "offends basic concepts of the criminal justice system." "[T]he rule's costly toll upon truth-seeking and law enforcement objectives presents a high obstacle for those urging [its] application."

Herring v. United States, 555 U.S. 135, 141 (2009) (citations omitted); see Hudson v. Michigan, 547 U.S. 586, 591 (2006); Washington v. Commonwealth, 60 Va. App. 427, 435-36, 728 S.E.2d 521, 525-26 (2012). See also Davis v. United States, 131 S. Ct. 2419, 2426-28 (2011).

Furthermore, binding case law plainly states, "'The deterrent purpose of the exclusionary rule necessarily assumes that the police have engaged in willful, or at the very least negligent,

conduct which has deprived the defendant of some right.'" Knight v. Commonwealth, 61 Va. App. 297, 311, 734 S.E.2d 716, 723 (2012) (quoting Michigan v. Tucker, 417 U.S. 433, 447 (1974)); see Herring, 555 U.S. at 144 ("As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.").

In this case, the police clearly did not engage in any conduct that ought to be deterred through the application of the exclusionary rule. Indeed, as the trial court here correctly found, "the police did not act in an improper manner to obtain information from the defendant's computer." The parties even *stipulated* that the police "did not 'hack' or otherwise use nefarious means to gain access to the defendant's computer, but did so through a modified version of the software that the defendant had downloaded and was using." Sergeant Anders specifically stated in his affidavit in support of a search warrant of appellant's residence that the law enforcement version of Shareaza that he had used in his investigation had been modified in a manner so that it "eliminate[ed] any potential *private intrusion* on the suspect IP's computer or files." (Emphasis added). Therefore, in other words, the record establishes that, when Sergeant Anders accessed and viewed the child pornography files on appellant's computer, he did not do so by taking any action that a member of *the public* could not also have taken in accessing and viewing those files. In this respect, the law enforcement version of Shareaza that Sergeant Anders used was like the version of Shareaza that any member of the public could use, in that it could access any files that another Shareaza user had made publicly available – intentionally or inadvertently – for sharing

Simply put, by downloading Shareaza, a program *designed to facilitate the sharing of files*, appellant opened his shared files to any other person – law enforcement or otherwise. Sergeant Anders viewed appellant's incriminating files (like anyone else using Shareaza could

do), and then the police properly obtained and executed a search warrant at appellant's home, where more incriminating evidence was discovered. On this record, contrary to appellant's argument on appeal, appellant certainly was not entitled to the suppression of evidence under the exclusionary rule.

III. CONCLUSION

The record establishes that appellant installed file-sharing software onto his computer – the very purpose of which is to share files with other users of the same software. Even though appellant claimed to be under the impression that he had applied settings that would prevent others from accessing his computer files, law enforcement – through a means available to any member of the public – was nonetheless able to access appellant's files depicting child pornography. In addition, the record establishes that appellant was not surprised when police officers arrived at his residence, remarking that he had even "been waiting for y'all [the police] to come." Viewing the evidence in the light most favorable to the Commonwealth, as we must since it was the prevailing party below, the circumstances here do not establish a reasonable expectation of privacy by appellant in the contents of the incriminating files that appellant actually shared via the Shareaza software – and certainly do not require exclusion of the child pornography seized from appellant's computer. The trial court did not err in denying appellant's motion to suppress that evidence, and, accordingly, we affirm appellant's twenty convictions for possession of child pornography.

Affirmed.