COURT OF APPEALS OF VIRGINIA

Present: Judges Frank, Kelsey and Senior Judge Overton
Argued by teleconference

RAY KROMER

v. Record No. 1900-04-2

COMMONWEALTH OF VIRGINIA

OPINION BY
JUDGE ROBERT P. FRANK
JUNE 14, 2005

FROM THE CIRCUIT COURT OF THE CITY OF RICHMOND
Beverly W. Snukals, Judge

Jennifer M. Newman (C. David Whaley; Morchower, Luxton & Whaley, on brief), for appellant.

Kathleen B. Martin, Assistant Attorney General (Judith Williams Jagdmann, Attorney General, on brief), for appellee.

Ray Kromer, appellant, was convicted, in a bench trial, of fifteen counts of misdemeanor possession of child pornography in violation of Code § 18.2-374.1:1.[1] On appeal, he contends the evidence was insufficient to sustain his convictions. We hold the evidence was sufficient and affirm.

BACKGROUND

On March 26, 2003, Richmond police responded to a fire at a residence on Hanover Avenue in Richmond. After finding chemicals and explosives on the second floor, police called Special Agent Robert Ritchie of the F.B.I. to "take a look at the scene." Ritchie, a bomb technician, questioned appellant about the materials. Appellant responded that he "was making pyrotechnic devices, rockets and other pyrotechnic type devices." Appellant gave written

[1] Such an offense is now a Class 6 felony. The offense was a Class 1 misdemeanor on March 26, 2003, the date alleged in the indictments.

consent for police to search the residence. Concerned about terrorism, Ritchie also wanted to examine the contents of a computer located inside the residence for "explosive recipes" and possible visits to websites that "might indicate he [appellant] was making explosive mixtures and not just pyrotechnic mixtures." Appellant consented to a search of the computer.

Police removed the explosives and the computer on March 27, 2003. After initially securing the residence on March 26, 2003, police guarded the residence until the next day when officers removed the computer. They did not see anyone come or go during that time. According to Ritchie, appellant gave his father a key to the residence "so he [appellant] could still get into the house after he was released."

Police took the computer to Officer Jeff Deem, a computer forensics specialist. Deem examined the computer in June 2003 for bomb-related information. He began by removing the hard drive and creating a "true and accurate copy of the media." Deem found information concerning child pornography and obtained a second search warrant before examining the computer further.

Deem conducted a forensic examination of the computer using Ncase software and certain key words connected to child pornography such as "lolita" and "underage." He received more than one hundred hits. He looked for files or photographs, and located numerous images that were possibly child pornography.

Deem identified fifteen photographs at trial as being the ones he recovered from the computer. Each picture was labeled with its file name as well as the path to the file's location on the computer. Deem testified the files were downloaded sometime between December 28, 2002 and January 3, 2003. The pictures were located in a file-sharing program called "KaZaA." The folder appeared on a desktop shortcut link titled "my shared folder." The folder contained files such as "kids/girl13yearsold.jpg" and "11_11and 13yearand mom.jpg." The default setting for

KaZaA is to share files with other users via the Internet, although this computer's setting had been manipulated not to share files. Deem testified that there was no way to tell who downloaded the pictures or who used the computer at any given time.

Deem testified that the "systems registry" showed "R. Clark Kromer" was a registered owner of the Windows XP software. Another application on the computer showed a user name of "clarkkromer." The computer was not password protected, and anyone could have access to it. Deem testified that there is no evidence to suggest that anyone other than appellant used the computer.

Kenneth Pew, an electrical engineer, testified that accessing the photographs was a six-step process and that there were over five hundred photographs on the photo directory. Pew could not testify about the shortcut link on the desktop because he did not have the hardware to examine the actual desktop. However, in addressing the issue of desktop icons, he testified that when one opened a desktop link, a list of files within that folder would appear on the screen.

Appellant made a motion to strike the Commonwealth's evidence, arguing that there was no evidence that appellant owned or used the computer at the time that the images were downloaded. Appellant conceded that the images were taken from the computer. The court denied the motion, finding that under a "totality of the circumstances" approach, the evidence was sufficient to find appellant guilty beyond a reasonable doubt.

ANALYSIS

Appellant argues that the evidence at trial was insufficient to convict him of possession of child pornography. Specifically, he contends that the Commonwealth failed to prove he

knowingly possessed the images contained within the computer.[2] For the reasons that follow, we affirm.

In order to convict a person of possession of child pornography, the Commonwealth must prove beyond a reasonable doubt that the individual "knowingly possesse[d] sexually explicit visual material utilizing or having as a subject a person less than 18 years." Code § 18.2-374.1:1. Appellant correctly points out that this statute does not define possession, nor does any opinion of Virginia's appellate courts. Thus, in this case of first impression, we must define "possession" in the context of computer electronics, Internet technology, and intangible images.

We take guidance from the federal case of United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002), cert. denied, 537 U.S. 1223 (2003). The appellant in Tucker was convicted of one count of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). The government's computer expert discovered child pornography files on both the hard drive and in the cache files of Tucker's computer. Tucker conceded that he knew that when he visited a Web page, the images on that page would be sent to his browser's cache and thereby saved on his hard drive. Id. at 1204.

The Tucker court found that Tucker had control over the files present in his Web browser cache file. Id. The court held:

> Tucker . . . intentionally sought out and viewed child pornography knowing that the images would be saved on his computer. Tucker may have wished that his Web browser did not automatically cache viewed images on his computer's hard drive, but he concedes he knew the Web browser was doing so. Tucker continued to view child pornography knowing that the pornography was being saved, if only temporarily, on his computer. In such circumstances, his possession was voluntary. Since he knew his browser cached the

[2] Appellant does not dispute that the images were sexually explicit, the subjects being less than eighteen years of age.

> image files, each time he intentionally sought out and viewed child pornography with his Web browser he knowingly acquired and possessed the images.

Id. at 1205 (footnote omitted).

While the facts in Tucker differ from the facts here, we adopt the court's definition of possession of computer images. There is no question here that the images were downloaded and saved, and even linked to the desktop through a shortcut. We, therefore, begin with the premise that someone here "sought out" child pornography. It is clear that someone "acquired" the offensive images and brought them into appellant's home from "cyberspace." See United States v. Perez, 247 F. Supp. 2d 459, 484 n.12 (S.D.N.Y. 2003) (noting that without evidence that pornography was specifically downloaded and saved to a defendant's computer, the offending images "'may well have been located in cyberspace, not in [the defendant's] home'" (quoting United States v. Zimmerman, 277 F.3d 426, 435 (3d Cir. 2002))). Thus, our inquiry is one of who possessed the images after they were already procured. Our analysis is whether the evidence sufficiently connects the appellant to the computer and the images.

While this appears to be a case consigned to the new and evolving area of computer technology, we examine this case under familiar principles of constructive possession of contraband. We do not need to determine whether appellant was the person who downloaded the pornographic images, rather, we determine whether appellant knew the images existed and, if so, did he exercise dominion and control over them after they were downloaded?[3]

When the sufficiency of the evidence is challenged on appeal, we review the evidence "in the light most favorable to the Commonwealth, granting to it all reasonable inferences fairly deducible therefrom." Bright v. Commonwealth, 4 Va. App. 248, 250, 356 S.E.2d 443, 444

[3] We note that while the evidence shows that the images were downloaded between December 28, 2002 and January 3, 2003, the appellant was charged with possessing the images on March 26, 2003.

(1987). The trial court's judgment will not be set aside unless plainly wrong or without evidence to support it. Josephs v. Commonwealth, 10 Va. App. 87, 99, 390 S.E.2d 491, 497 (1990) (*en banc*). Under this standard, "a reviewing court does not 'ask itself whether *it* believes that the evidence at the trial established guilt beyond a reasonable doubt.'" Myers v. Commonwealth, 43 Va. App. 113, 118, 596 S.E.2d 536, 538 (2004) (citation omitted and emphasis in original). It asks instead whether "'*any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" Kelly v. Commonwealth, 41 Va. App. 250, 257, 584 S.E.2d 444, 447 (2003) (quoting Jackson v. Virginia, 443 U.S. 307, 319 (1979)) (emphasis in original). Thus, we do not "substitute our judgment for that of the trier of fact" even if our opinion were to differ. Wactor v. Commonwealth, 38 Va. App. 375, 380, 564 S.E.2d 160, 162 (2002).

In order to convict a person of illegal possession of contraband, "proof of actual possession is not required; proof of constructive possession will suffice." Maye v. Commonwealth, 44 Va. App. 463, 483, 605 S.E.2d 353, 363 (2004). To support a conviction based upon constructive possession, "the Commonwealth must point to evidence of acts, statements, or conduct of the accused or other facts or circumstances which tend to show that the defendant was aware of both the presence and character of the [contraband] and that it was subject to his dominion and control." Drew v. Commonwealth, 230 Va. 471, 473, 338 S.E.2d 844, 845 (1986) (citation omitted). Ownership or occupancy of the premises on which the contraband was found is a circumstance probative of possession. Archer v. Commonwealth, 26 Va. App. 1, 12, 492 S.E.2d 826, 832 (1997).

"Circumstantial evidence is as competent and is entitled to as much weight as direct evidence, provided it is sufficiently convincing to exclude every reasonable hypothesis except that of guilt." Breeden v. Commonwealth, 43 Va. App. 169, 177, 596 S.E.2d 563, 567 (2004).

"The Commonwealth is not required to prove that there is no possibility that someone else may have planted, discarded, abandoned or placed the [contraband]" where the contraband is discovered. Brown v. Commonwealth, 15 Va. App. 1, 10, 421 S.E.2d 877, 883 (1992) (*en banc*). "To resolve the issue, the Court must consider the totality of the circumstances established by the evidence." Williams v. Commonwealth, 42 Va. App. 723, 735, 594 S.E.2d 305, 311 (2004).

Appellant's reasonable hypothesis of innocence is that others, family members or friends, could have used the computer and downloaded the images. As we earlier indicated, whether appellant or someone else downloaded the images is not determinative of our analysis. The issue is whether appellant knowingly possessed the images after they were previously downloaded into the computer. The issue of who originally procured the offensive images is of no concern to our analysis.

The trial court found that appellant had exclusive control of the residence. Appellant gave consent to search the residence, and he admitted ownership of certain pyrotechnics found on the premises. The court further found "the registration on the computer tied to his name," along with appellant's name being associated with the computer during the time when the computer made one hundred "hits" on child pornography. The court concluded that, most importantly, the computer had "quick desktop access" to the folder containing the images. Using a totality of the circumstances approach, the court found the evidence sufficient to show appellant had control of the residence and the computer.

We conclude that the evidence supports the trial court's findings. There is no dispute that the computer contained pornographic images in a KaZaA shared file that could be easily accessed through a desktop link. The computer was seized from a residence to which appellant had a key. Appellant gave a key to his father so that he would be able to enter the premises at a later date, indicating that appellant had control over the residence. Appellant also admitted that

the chemical mixtures were his and that he was making "pyrotechnic devices" at the residence. The police did not see anyone else come to or go away from the residence from March 26 until they completed their search on March 27. The reasonable inference is that appellant lived at this residence.

The systems registry on the computer revealed "R. Clark Kromer" as a registered owner of the Windows XP software. Another application showed a user name of "clarkkromer." The KaZaA software default setting had been manually set to disallow file sharing, establishing the user's control and management of the files. The evidence showed that the files had been downloaded between December 28, 2002 and January 3, 2003. The desktop shortcut, entitled "my shared folder," created easy access to files such as "kids/girl13yearsold.jpg" and "11_11and 13yearand mom.jpg," making the existence of those files obvious to anyone who clicked on that link. The images, accessible to the user through that desktop shortcut, were conveniently located and readily viewable. The record supports the reasonable inference that appellant used the computer and had knowledge and control over its contents.

Appellant cites Perez, for the proposition that "one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically stored in the browser's cache, without having purposely saved or downloaded the image." Appellant did not contest at trial that the images were deliberately downloaded into the computer. Because appellant did not make this argument below, we will not consider it for the first time on appeal. See Rule 5A:18; see also Buck v. Commonwealth, 247 Va. 449, 452-53, 443 S.E.2d 414, 417 (1994) (holding that the same argument must have been raised, with specificity, at trial before it can be considered on appeal).

We are not suggesting that anyone who ever uses a computer containing sexually explicit images of children is guilty of possessing child pornography. Here, the reasonable inference is

that appellant owned the residence and was the user/owner of the computer. While appellant contends the images were "hidden" in the computer, the facts defeat his argument. The desktop shortcut indicates that the appellant manipulated the images to be easily accessible and continuously available. Under the specific facts of this case, it is clear that appellant possessed the computer and the images contained therein.

For the foregoing reasons, the decision of the trial court is affirmed.

Affirmed.