No. 98808
Court of Appeals of Ohio EIGHTH APPELLATE DISTRICT COUNTY OF CUYAHOGA

State v. Diaz

2013 Ohio 1449
Decided Apr 11, 2013

No. 98808

04-11-2013

STATE OF OHIO PLAINTIFF-APPELLEE v. CARLOS DIAZ DEFENDANT-APPELLANT

ATTORNEY FOR APPELLANT Michael J. Manuszak ATTORNEYS FOR APPELLEE Timothy J. McGinty Cuyahoga County Prosecutor By: Denise J. Salerno Assistant Prosecuting Attorney

SEAN C. GALLAGHER

JOURNAL ENTRY AND OPINION

JUDGMENT:
AFFIRMED

Criminal Appeal from the
Cuyahoga County Court of Common Pleas
Case No. CR-532195

2 **BEFORE:** S. Gallagher, P.J., Rocco, J., and McCormack, J. *2

ATTORNEY FOR APPELLANT

Michael J. Manuszak

ATTORNEYS FOR APPELLEE

Timothy J. McGinty
Cuyahoga County Prosecutor
By: Denise J. Salerno
Assistant Prosecuting Attorney

3 *3 SEAN C. GALLAGHER, P.J.:

{¶1} Defendant-appellant, Carlos Diaz ("defendant"), was convicted, after a bench trial, of 32 counts[1] of pandering sexually oriented matter involving a minor with forfeiture specifications and one count of possessing criminal tools, also with a forfeiture specification. In this appeal, he contends that his convictions were based upon insufficient evidence. For the reasons that follow, we affirm.

[1] Eight counts involved violations of R.C. 2907.322(A)(2), and the remaining counts involved violations of R.C. 2907.322(A)(1). All counts are felonies of the second degree.

{¶2} Defendant presents two assignments of error, which we address together because they involve the same analysis of law and fact.

Assignment of Error No. 1

> The trial court erred in denying Appellant's Rule 29 Motion for Acquittal where there was insufficient evidence to identify the Appellant as the perpetrator of the crimes herein.

> **Assignment of Error No. 2**

> The trial court erred in finding Appellant guilty under O.R.C. §2903.322(A)(1) & (2) in trading, online downloading and online distribution and disseminating of videos and photographs of child pornography, particularly by way of downloading child pornographic video through file sharing networks.

{¶3} In both assignments of error, defendant argues that the state's evidence was insufficient to support his convictions. Defendant believes there was insufficient evidence as to his identity as the perpetrator of the crimes. He also contends that the *4 state did not establish that he knew there was peer-to-peer software on his computer equipment or that his computer was used to advertise or disseminate the prohibited material.

{¶4} When an appellate court reviews a claim of insufficient evidence, "'the relevant inquiry is whether, after viewing the evidence in a light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime proven beyond a reasonable doubt.'" *State v. Leonard,* 104 Ohio St.3d 54, 2004-Ohio-6235, 818 N.E.2d 229, ¶ 77, quoting *State v. Jenks,* 61 Ohio St.3d 259, 574 N.E.2d 492 (1991), paragraph two of the syllabus. A motion for acquittal under Crim.R. 29(A) is governed by the same standard used for determining whether a verdict is supported by sufficient evidence. *State v. Tenace,* 109 Ohio St.3d 255, 2006-Ohio-2417, 847 N.E.2d 386, ¶ 37.

{¶5} The applicable standard requires a determination as to whether there was any evidence that, if believed, would support convictions against defendant for violations of R.C. 2907.322(A)(1) and (2), which provide:

> (A) No person, with knowledge of the character of the material or performance involved, shall do any of the following:
> (1) Create, record, photograph, film, develop, reproduce, or publish any material that shows a minor participating or engaging in sexual activity, masturbation, or bestiality;
> (2) Advertise for sale or dissemination, sell, distribute, transport, disseminate, exhibit, or display any material that shows a minor participating or engaging in sexual activity, masturbation, or bestiality[.]

5 *5

{¶6} Rick McGinnis ("McGinnis") is an investigator assigned to Ohio's Internet Crimes Against Children Task Force ("ICAC"). He participated in the investigation that led to defendant's arrest in this case, and he utilized law enforcement software known as Peer Spectre.

{¶7} Peer Spectre is a search program that operates on the Gnutella network, which is a public peer-to-peer network where people share their computer files back and forth. The Gnutella network enables people to log onto the Internet to search, find, retrieve, and download shared files from other computers, including child pornography. The search will reveal an IP address and SHA1 values,[2] and from this information, the user can download the desired file from the computer(s) that offered to share it. Peer Spectre conducts an automated search that identifies file sharing of known or suspected child pornography associated with a specific IP address.

[2] SHA1 stands for Secure Hash Algorithm 1, which consists of 32 digits and functions as a file's digital signature or unique identifier, which cannot be altered. McGinnis testified that SHA1 values are accurate in identifying a file to the 160th degree, which is "better than DNA." There is a certainty exceeding 99.99 percent that two or more files with the same SHA1 value are identical copies of the same file regardless of the file name. If any part of a file is altered in any way, the SHA1 is changed.

{¶8} Each time that Peer Spectre is used by a law enforcement agency anywhere in the world, the results are compiled in a centralized server. The information that is logged into the central database includes the IP address, the port that it came from, and the date and time of the search. Law enforcement agencies are then enabled to query the information that Peer Spectre recorded into the central server. *6

6

{¶9} McGinnis identified state's exhibit No. 1 as being an IP activity report, which references a specific IP address, SHA1 values, and contains dates ranging from April 28, 2009 to May 6, 2009. From that, he was able to identify movies and images of child pornography being associated with that IP address. McGinnis created state's exhibit No. 13, which is a disk with copies of the child pornography files that he had identified from state's exhibit No. 1.

{¶10} After a few of the videos were played in open court, the defense stipulated that state's exhibit No. 13 showed "a minor participating or engaging in sexual activity, masturbation or bestiality" for purposes of Counts 1 through 31 of the indictment. However, the defense did not stipulate that the videos and images belonged to defendant or that he had recorded them.

{¶11} McGinnis learned, from records subpoenaed from Time Warner, that defendant's son, Randy, was the subscriber for the relevant IP address. Randy's address was an apartment in Brook Park, Ohio. Police conducted surveillance of that residence and obtained a search warrant. McGinnis participated in executing the search warrant on September 10, 2009, at 9:19 a.m. During the search, the following items were seized: an Enermax black computer, a Buffalo hard drive, and a Hitachi hard drive.

{¶12} McGinnis testified that the files identified by Peer Spectre are located in a person's computer in a "shared file" after being downloaded from the Gnutella network.

{¶13} Luis Vargas testified that defendant is related to Vargas's stepfather. Vargas calls defendant his uncle. Vargas had spent the night at defendant's residence on five or *7 six occasions in 2009 with his cousin Julio. Vargas and Julio were about 12 and 15 years old, respectively. Defendant lived at the apartment in Brook Park that was the subject of the search warrant in this case. Vargas said defendant lived alone in this one-bedroom apartment. Defendant had a computer in his bedroom and would show the boys adult pornography. Defendant

7

would not allow the boys to use his computer. Although defendant told Vargas he "didn't have the internet," Vargas testified that he saw defendant accessing YouTube and Google. Vargas never saw anyone besides defendant using the computer.

{¶14} Investigator Rice is an investigator with the Cuyahoga County Prosecutor's office and is assigned to the ICAC task force. He is trained as a computer forensic examiner, and the defense stipulated to his expertise in computer forensic analysis. He participated in the investigation in this case and was present at the search of the residence in September 2009. Investigator Rice testified that child pornography was found on several computer drives that were seized during the search. He was able to determine the file names, the date they were created on the computer hard drive, and when each was last accessed from that computer. For example, one file on the Western Digital hard drive was created on May 11, 2009, at 1:48 p.m. and was last accessed on August 13, 2009, at 7:30 p.m. The defense stipulated to the contents of the videos as involving children engaging in sexual activity for purposes of Counts 9 through 32.

{¶15} Investigator Rice also found file-sharing programs on the equipment seized from the residence. When
8 LimeWire is installed, it creates a folder that is called *8 "shared." This is the file that is used when a person is
online to connect with, and share content, with other peers. "Carlos port" was the file path associated with it on the hard drive. Investigator Rice also found FrostWire, another file-sharing program, on an HP Pavilion desktop computer.

{¶16} During cross-examination, Investigator Rice indicated that it is possible for viruses to be placed in people's files where data can be disguised and sent without the recipient's knowledge of its content unless they opened it. In this case, the child pornography files were downloaded, accessed again at later times, and none of them had been deleted.

{¶17} Investigator Rice confirmed that persons with proper training and skill can hack into computers and place things on other people's computers without their knowledge. Investigator Rice has seen computers that have been remotely accessed, which leaves artifacts that evidence the remote access. He used the Forensic Tool Kit created by AccessData to determine whether defendant's equipment had been remotely accessed. Investigator Rice did not find any artifacts or evidence that defendant's equipment had been remotely accessed by anyone.

{¶18} In this case, there was no evidence that someone else was using defendant's wireless connection without his knowledge because the actual files were found on his equipment.

{¶19} Detective Jamie Bonnette assisted in the execution of the search warrant. He interviewed defendant, who
9 denied any knowledge of child pornography on the *9 computers. There was a woman present in the home who
did not speak or understand English. Defendant initially said she lived with him but later said she did not. Det. Bonnette felt it was possible that she did live there. Defendant also indicated a man named Emanuel Rivera lived in the apartment previously but had moved to Puerto Rico. Defendant said his son, Randy, had not lived in the apartment for a year.

{¶20} Defendant said he had two computers: a laptop and a PC. He told Det. Bonnette that he was the only person who used the computers. Defendant denied using FrostWire or LimeWire and said he did not use them because they caused viruses. Det. Bonnette felt that defendant was being evasive.

{¶21} The court denied defendant's motion for acquittal and rendered its verdict finding defendant guilty on all counts. The court noted that defendant's primary defense was that he was not the person who imported or placed the child pornography on the computers. The court found that the state had proved that he was the person who downloaded the child pornography beyond a reasonable doubt. The court referred to some evidence in support of this finding, including that defendant had told police he lived alone. The court also cited Vargas's testimony, which indicated the defendant did not allow him to use the computer and Vargas only saw defendant using the computer. While there was some evidence that other people had lived in the apartment, the court expressed "no substantial belief that they had any access to the computer."

{¶22} The evidence establishes that the child pornography files were downloaded and re-accessed at a later
10 time. That fact, coupled with the evidence that defendant was *10 the only person who used the computers,
provided evidence as to defendant's knowledge of the child pornography contents of the files.

{¶23} While defendant suggests that a computer virus could have caused the child pornography to be placed on his computer without his knowledge, there is no evidence to support this theory. The computers were searched for evidence of remote access, and none was found.

{¶24} There was sufficient evidence to support appellant's convictions, and his assignments of error are overruled.

{¶25} Judgment affirmed.

It is ordered that appellee recover from appellant costs herein taxed.

The court finds there were reasonable grounds for this appeal.

It is ordered that a special mandate issue out of this court directing the common pleas court to carry this judgment into execution. The defendant's convictions having been affirmed, any bail pending appeal is terminated. Case remanded to the trial court for execution of sentence.

A certified copy of this entry shall constitute the mandate pursuant to Rule 27 of the Rules of Appellate Procedure. SEAN C. GALLAGHER, PRESIDING JUDGE KENNETH A. ROCCO, J., and
TIM McCORMACK, J., CONCUR