

NOTICE: SLIP OPINION
(not the court’s final written decision)

The opinion that begins on the next page is a slip opinion. Slip opinions are the written opinions that are originally filed by the court.

A slip opinion is not necessarily the court’s final written decision. Slip opinions can be changed by subsequent court orders. For example, a court may issue an order making substantive changes to a slip opinion or publishing for precedential purposes a previously “unpublished” opinion. Additionally, nonsubstantive edits (for style, grammar, citation, format, punctuation, etc.) are made before the opinions that have precedential value are published in the official reports of court decisions: the Washington Reports 2d and the Washington Appellate Reports. An opinion in the official reports replaces the slip opinion as the official opinion of the court.

The slip opinion that begins on the next page is for a published opinion, and it has since been revised for publication in the printed official reports. The official text of the court’s opinion is found in the advance sheets and the bound volumes of the official reports. Also, an electronic version (intended to mirror the language found in the official reports) of the revised opinion can be found, free of charge, at this website: <https://www.lexisnexis.com/clients/wareports>.

For more information about precedential (published) opinions, nonprecedential (unpublished) opinions, slip opinions, and the official reports, see <https://www.courts.wa.gov/opinions> and the information that is linked there.

FILED
APRIL 9, 2015
In the Office of the Clerk of Court
WA State Court of Appeals, Division III

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON
DIVISION THREE

STATE OF WASHINGTON,)	No. 32058-8-III
)	
Respondent,)	
)	
v.)	OPINION PUBLISHED
)	IN PART
CASEY D. PEPPIN,)	
)	
Appellant.)	

LAWRENCE-BERREY, J. — A trial court found Casey Peppin guilty of three counts of first degree possession of depictions of a minor engaged in sexually explicit conduct. In this appeal, Mr. Peppin challenges the trial court’s denial of his motion to suppress the images of child pornography found on his computer. He raises an issue of first impression in Washington. He contends that law enforcement’s use of enhanced peer to peer file sharing software to remotely access the shared files on his computer was illegal under the Fourth Amendment of the United States Constitution and article I, section 7 of the Washington State Constitution. He maintains that such conduct represents an intrusion into his private affairs because he had a reasonable expectation of privacy in his personal computer files. We hold that Mr. Peppin did not have a constitutionally

No. 32058-8-III

State v. Peppin

protected privacy right in the image files he shared with the public. We therefore affirm his convictions.

FACTS

On December 29, 2011, Spokane Detective Brian Cestnik conducted an online investigation of the Gnutella network to identify persons possessing and sharing child pornography. Using peer to peer software called Round Up version 1.5.3, Detective Cestnik found child pornography on Mr. Peppin's computer in a shared folder.

Detective Cestnik's report of the investigation explains peer to peer file sharing. According to his report, peer to peer file sharing is a method of Internet communication that allows users to share digital files. User computers link together to form a network; the network allows direct transfer of shared files from one user to another. Peer to peer software applications allow users to set up and share files on the network with others using compatible peer to peer software. For instance, LimeWire and Shareaza are software applications that allow users to share files over the Gnutella network.

To gain access to shared files, a user must first download peer to peer software, which can be found on the Internet. Then, the user opens the peer to peer software on his or her computer and conducts a keyword search for files that are currently being shared on the network. The results are displayed and the user selects a file for download. The

No. 32058-8-III

State v. Peppin

downloaded file is transferred through a direct connection between the computer wishing to share the file and the user's computer requesting the file. The Gnutella network gives users the ability to see a list of all files that are available for sharing on a particular computer.

For example, a person interested in obtaining child pornographic images opens the peer to peer software application on his or her computer and conducts a file search using keyword terms such as "preteen sex." The search is sent out over the network of computers to those using compatible peer to peer software. The results of the search are returned and displayed on the user's computer. The user selects the file he or she wishes to download. The file is then downloaded directly from the host computer onto the user's computer. The downloaded file is stored on the user's computer until moved or deleted.

When more than one host computer offers the file that is requested, peer to peer software allows the user to download different parts of the file from different computers. This speeds up the time it takes to download a file. For instance, a person using Shareaza to download an image may actually receive parts of the image from multiple computers. However, often a user downloading an image file receives the entire image from one computer.

No. 32058-8-III

State v. Peppin

Every file shared on the Gnutella network has a unique identifier based on a Secure Hash Algorithm (SHA1) value, sometimes called a hash value. The SHA1 value acts as a fingerprint for that file. It is computationally infeasible for two files with different content to have the same SHA1 hash value.

A peer to peer file transfer is assisted by reference to an Internet Protocol (IP) address. In general, the numeric IP address is unique to a particular computer during an online Internet session. The IP address provides a location, making it possible for data to be transferred between computers. Investigators can search public records on the Internet to determine which Internet provider is assigned the IP address. Investigators can contact the Internet provider and gain information about the user based on the IP address assigned to the computer.

Detective Cestnik searched the Gnutella network for “pthc,” the commonly used term for preteen hard core Internet pornography. Clerk’s Papers (CP) at 17. The results indicated that images matching the search terms could be found on a host computer with an IP address linked to Spokane. Detective Cestnik’s check of the IP address through two different Internet search engines confirmed that the IP address was in Spokane and that Qwest Communications was the provider.

No. 32058-8-III

State v. Peppin

Detective Cestnik used the IP address to access the host computer. The host computer was configured to allow browsing of its shared folder. Detective Cestnik viewed the contents of the folder and noticed four files that appeared to be child pornography. Detective Cestnik successfully downloaded three files from the host computer before it stopped. After reviewing the videos in the files, he determined that each video constituted possession or dealing in depictions of minors engaged in sexually explicit conduct.

Detective Cestnik presented Qwest Communications with a search warrant requesting information on the IP address for the host computer. Qwest Communications advised Detective Cestnik that the IP address was connected to Mr. Peppin and provided Mr. Peppin's address.

Detective Cestnik then obtained a search warrant for Mr. Peppin's computer. A complete forensic investigation uncovered over 100 videos of what appeared to be minors engaged in sexually explicit conduct. The State charged Mr. Peppin by amended information with three counts of first degree possession of depictions of minors engaged in sexually explicit conduct and one count of first degree dealing in depictions of minors engaged in sexually explicit conduct.

No. 32058-8-III

State v. Peppin

Mr. Peppin moved to suppress the computer files downloaded by Detective Cestnik during his Internet search. He maintained that law enforcement's access and download of his computer files via the Internet was an intrusion into his private affairs and an unlawful warrantless search. At the suppression hearing, Mr. Peppin also argued that the use of enhanced peer to peer software provided information to law enforcement that was not available to the general public.

At the hearing, in addition to the report provided by Detective Cestnik, the court heard from Mr. Peppin's expert, Jennifer McCamm. Ms. McCamm worked as a computer system administrator, with some background in computer forensics. Ms. McCamm testified that the purpose of peer to peer file sharing programs is to share files. She explained that sharing is inherent in these programs and a user must change the default setting if they desire not to share files.

Ms. McCamm said that she had not seen the law enforcement peer to peer software. Still, she testified that law enforcement uses an enhanced version of peer to peer software that is different from what is available to the general public. As the biggest difference, she noted that law enforcement software has features that make searching the network easier. For instance, law enforcement software can search all user files on the Gnutella network, regardless of what client interface is being used. Also, the software

No. 32058-8-III

State v. Peppin

provides law enforcement with a computer's IP address and gives the ability to identify files by hash value. Last, the software is built to do single source downloads. Despite this testimony, Ms. McCamm repeated that she had never tested or interacted with this software in any form.

The trial court denied Mr. Peppin's motion to suppress. The court found that under both article I, section 7 of the Washington State Constitution and the Fourth Amendment to the United States Constitution, Mr. Peppin had no reasonable expectation of privacy or trespass protection when using file sharing software.

After a bench trial, the court returned guilty findings for the three counts of first degree possession of depictions of minors engaged in sexually explicit conduct. The court returned a finding of not guilty on the one count of dealing in the depictions of minors engaged in sexually explicit conduct. The court declined Mr. Peppin's request for an exceptional sentence downward. The court imposed a low-end standard range sentence of 46 months.

ANALYSIS

Whether Mr. Peppin had a constitutionally protected privacy right in the image files he shared with the public

The Fourth Amendment to the United States Constitution prohibits unreasonable search and seizures. The Washington State Constitution offers broader protection of

No. 32058-8-III

State v. Peppin

privacy than the United States Constitution. *State v. Carter*, 151 Wn.2d 118, 125, 85 P.3d 887 (2004). Article I, section 7 of the Washington State Constitution provides, “No person shall be disturbed in his private affairs, or his home invaded, without authority of law.”

“[U]nder the Washington Constitution, the inquiry focuses on ‘those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass absent a warrant.’” *State v. Young*, 123 Wn.2d 173, 181, 867 P.2d 593 (1994) (quoting *State v. Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151 (1984)). The interpretation and application of article I, section 7 requires a two-part analysis. *State v. Puapuaga*, 164 Wn.2d 515, 522, 192 P.3d 360 (2008). “The first step requires us to determine whether the action complained of constitutes a disturbance of one’s private affairs. If there is no private affair being disturbed, the analysis ends and there is no article I, section 7 violation. If, however, a private affair has been disturbed, the second step is to determine whether authority of law justifies the intrusion. Authority of law may be satisfied by a valid warrant.” *Id.*

Whether a person’s affairs are private is not judged by the person’s subjective expectation of privacy, but is determined in part by the historical treatment of the interest asserted. *Id.* If there is no historical evidence of protection under article I, section 7, then

No. 32058-8-III

State v. Peppin

the relevant inquiry is whether the expectation is one that a citizen of this state is entitled to hold. *Id.* “This part of the inquiry includes a look into the nature and extent of the information that may be obtained as a result of the governmental conduct and the extent to which the information has been voluntarily exposed to the public.” *Id.*

Federal circuit courts have consistently held that a person who installs and uses file sharing software does not have a reasonable expectation of privacy in the files to be shared on his or her computer. See *United States v. Ganoë*, 538 F.3d 1117, 1127 (9th Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008); *United States v. Stults*, 575 F.3d 834, 842-43 (8th Cir. 2009). *Ganoë* held that a defendant’s expectation of privacy in his or her personal computer does not “survive [his] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program.” *Ganoë*, 538 F.3d at 1127.

The Ninth Circuit in *United States v. Borowy*, 595 F.3d 1045 (9th Cir. 2010), addressed a situation identical to the one here. A law enforcement agent used LimeWire peer to peer software to monitor trafficking in child pornography. *Id.* at 1046. After conducting a keyword search, the agent used special software that verified the “hash marks” of files known to be images of child pornography. *Id.* At least one of these files was shared through what was later determined to be Mr. Borowy’s IP address. *Id.* The

No. 32058-8-III

State v. Peppin

officer used LimeWire to search the rest of the files being shared on Mr. Borowy's computer. *Id.* at 1046-47. The agent downloaded seven files, four of which were child pornography. *Id.* at 1047. Later, a search warrant executed on Mr. Borowy's home uncovered a large number of images and videos of child pornography. *Id.*

Mr. Borowy moved to suppress this evidence, arguing that the agent's activities in locating and downloading the files from LimeWire constituted a warrantless search and seizure without probable cause that violated his Fourth Amendment rights. *Id.* The Ninth Circuit upheld the lower court's denial of the motion and held that Mr. Borowy lacked a reasonable expectation of privacy in the shared files. *Id.* at 1047-48. The court concluded that Mr. Borowy's files were entirely exposed to the public view and available for download so his "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. Furthermore, the court also rejected Mr. Borowy's argument that the use of a publicly unavailable software program rendered the search unlawful. *Id.* The court concluded that Mr. Borowy had exposed the entirety of the files to the public, which negated any reasonable expectation of privacy in those files, and that the government's software simply functioned as a mechanism to sort through the shared files. *Id.* It is clear

No. 32058-8-III

State v. Peppin

from *Borowy* and other federal cases that Detective Cestnik's access of Mr. Peppin's shared files was not a violation the Fourth Amendment to the United States Constitution.

The broader protection of the Washington State Constitution also does not offer any relief to Mr. Peppin. Detective Cestnik's access of Mr. Peppin's computer through peer to peer software and download of the shared files was not a disturbance of Mr. Peppin's private affairs. Historically speaking, Washington courts have not afforded article I, section 7 protections to information voluntarily held out to the public. "[W]hat is voluntarily exposed to the general public and observable without the use of enhancement devices from an unprotected area is not considered part of a person's private affairs." *Young*, 123 Wn.2d at 182. Here, Mr. Peppin voluntarily offered public access to the computer files obtained by Detective Cestnik. Mr. Peppin used peer to peer software to make these shared files available without restriction. Anyone wanting to view or download the files could do so. Law enforcement's access of these files was not an intrusion into Mr. Peppin's private affairs.

Additionally, this is not the type of information that a citizen of this state is entitled to hold as private. The inherent nature of peer to peer software is the public sharing of digital computer files. Individuals using file sharing software cannot expect a privacy interest in files they hold open to the public. Again, Mr. Peppin's use of peer to peer file

No. 32058-8-III

State v. Peppin

sharing voluntarily opened this information to the public for anyone to access, including law enforcement. There is no disturbance of a person's private affairs when law enforcement accesses shared computer files that the person holds publically available for viewing and download. Thus, there is no violation within the context of article I, section 7 of the Washington Constitution.

Despite Mr. Peppin's argument, Detective Cestnik's use of specially designed software to search the peer to peer network did not transform his actions into an unlawful search. This situation is not like *Young*, where the Washington Supreme Court held that the use of an infrared device to gather information of the interior of a defendant's home was a warrantless invasion in his private affairs and his home. *Young*, 123 Wn.2d at 188.

In *Young*, the thermal infrared investigation was an invasion of privacy because it allowed law enforcement to peer into the walls of the home and reveal more than what was available to the naked eye. *Id.* at 183. Additionally, the use of the sense-enhancing device penetrated the constitutional line of privacy that encircled the home, thus invading the home for purposes of article I, section 7 of the Washington Constitution. *Id.* at 186.

Here, unlike *Young*, law enforcement did not gain more information than was available to the public. Detective Cestnik did not intrude into a computer file that Mr. Peppin intended to keep private. The files obtained by Detective Cestnik were ones that

No. 32058-8-III

State v. Peppin

Mr. Peppin made available to the public on the Gnutella network. Additionally, unlike *Young*, the peer to peer software was not an enhancement device that allowed law enforcement to view what was hidden to the public. Law enforcement simply used a more efficient method for finding this publicly shared information. The government's software allowed them to efficiently view what was already knowingly exposed to the public.

We conclude that a person's private affairs are not disturbed when law enforcement uses peer to peer software to view files that the person voluntarily shares with the public on his or her computer. The trial court properly denied Mr. Peppin's motion to suppress.

The remainder of this opinion has no precedential value. Therefore, it will be filed for public record in accordance with RCW 2.06.040, the rules governing unpublished opinions.

Statement of Additional Grounds for Review

Mr. Peppin raises three issues in his statement of additional grounds. First, he challenges the calculation of his offender score. He contends that the multiple counts of possession of depictions of minors engaged in sexually explicit conduct constituted the same criminal conduct.

No. 32058-8-III

State v. Peppin

Generally, “[w]hen imposing a sentence for two or more current offenses, the court determines the sentence range for each current offense by using all other current and prior convictions as if they were prior convictions for the purpose of the offender score.” *State v. Ehli*, 115 Wn. App. 556, 560, 62 P.3d 929 (2003) (footnote omitted). However, some or all current offenses can count as one crime if the court finds that those offenses encompass the same criminal conduct. RCW 9.94A.589(1)(a). “Same criminal conduct” means two or more crimes that require the same criminal intent, are committed at the same time and place, and involve the same victim. RCW 9.94A.589(1)(a).

Mr. Peppin’s challenge fails. The three counts do not constitute the same criminal conduct. The undisputed findings by the trial court show that each video depicts a different victim. When a defendant is convicted of multiple counts of depictions of minors engaged in sexually explicit conduct and the depictions are of different child victims, the current convictions do not count as the same criminal conduct. *See Ehli*, 115 Wn. App. at 560-61.

Second, Mr. Peppin contends that the trial court erred by denying his request for an exceptional sentence downward. He maintains that the trial court should have imposed a sentence below the standard range because he suffers from mental health problems as a result from a head injury.

No. 32058-8-III

State v. Peppin

A standard range sentence is generally not appealable. *State v. Khanteechit*, 101 Wn. App. 137, 138, 5 P.3d 727 (2000). However, where a defendant has requested an exceptional sentence below the standard range, the denial can be reviewed if the court “either refused to exercise its discretion at all or relied on an impermissible basis for refusing to impose an exceptional sentence.” *Id.* “[A] trial court that has considered the facts and has concluded that there is no basis for an exceptional sentence has exercised its discretion, and the defendant may not appeal that ruling.” *Id.* at 138-39 (quoting *State v. Garcia-Martinez*, 88 Wn. App. 322, 330, 944 P.2d 1104 (1997)).

Mr. Peppin may not appeal his standard range sentence because the trial court exercised its discretion during sentencing. The trial court considered Mr. Peppin’s brain injury and his request for an exceptional sentence downward. The court noted that a doctor diagnosed Mr. Peppin with recurrent major depression, generalized anxiety and masochistic personality traits, and that these disorders influenced Mr. Peppin’s behavior and poor decision-making. However, the court found that Mr. Peppin was not incompetent nor suffering from a major mental disorder that would make him unable to understand that what he was doing was wrong. To the contrary, the court recognized that when Mr. Peppin was arrested, he acknowledged that he knew his actions were wrong. Although sympathetic to Mr. Peppin’s circumstances, the trial court concluded that there

No. 32058-8-III

State v. Peppin


was no substantial and compelling reason to depart from the standard range sentence.

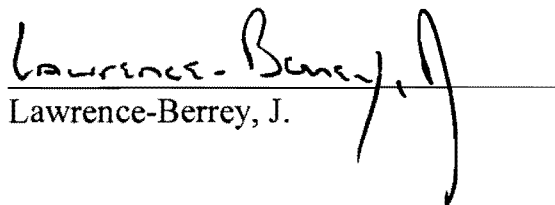
The trial court exercised its discretion. Thus, Mr. Peppin's standard range sentence is not reviewable.

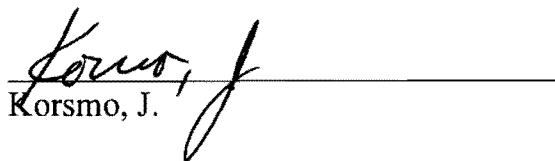
Third, Mr. Peppin calls attention to defense counsel's discussion with the trial court where counsel pointed out that the court failed to identify which video supported each charge. He asks this court to investigate whether an error took place. The trial court made explicit findings that identify the video or videos that support each count. The findings for each count names the video or videos that supported the count and described the depiction in the video. The court concluded that each of the videos in counts I, III, and IV depicted sexually explicit conduct as defined by RCW 9.68A.011(4). This court does not find any error in the issues raised by Mr. Peppin in his statement of additional grounds.

Affirm.

WE CONCUR:


Siddoway, C.J.


Lawrence-Berrey, J.


Korsmo, J.