

IN THE MISSOURI COURT OF APPEALS WESTERN DISTRICT

STATE OF MISSOURI,

Respondent,

v.

DAVID N.C. SACHS,

Appellant.

WD72821

Opinion filed: April 24, 2012

APPEAL FROM THE CIRCUIT COURT OF BOONE COUNTY, MISSOURI The Honorable Clifford E. Hamilton, Jr.

Before Division Two: Mark D. Pfeiffer, Presiding Judge, Joseph M. Ellis, Judge and Victor C. Howard, Judge

David Sachs appeals from his convictions on one count of possession of child pornography, § 573.035, and one count of promoting child pornography in the second degree, § 573.025. Specifically, Sachs challenges the admission of evidence recovered as a result of a warrantless search of his personal computer. For the following reasons, Appellant's convictions and sentences are affirmed.

On July 27, 2009, Sergeant Cavanaugh of the St. Louis County Police Department contacted Detective Andy Anderson of the Boone County Sherriff's Department about an ongoing child pornography investigation. Sergeant Cavanaugh had executed a search warrant at a Webster Groves home after obtaining evidence that the internet provider address ("IP address") associated with that home had been used in the past to upload and download child pornography. The owners of the home had informed Sergeant Cavanaugh that they had a son, Appellant, who currently lived in Columbia but had previously lived in the home and used the internet. Sergeant Cavanaugh asked Detective Anderson to interview Appellant.

Detective Anderson went to Appellant's apartment at 2900 Old Highway 63 along with Detective Tracy Perkins of the Boone County Sheriff's Department and Officer Purdy of the Columbia Police Department. When the officers knocked on the door, one of Appellant's two roommates answered the door. The apartment had three separate bedrooms with a shared common area, kitchen, and bathroom. When Detective Anderson asked if Appellant was home, the second roommate volunteered to go get him. After introducing himself, Detective Anderson asked to speak with Appellant in private, and they went to Appellant's bedroom to talk.

When they entered the room, Detective Anderson noticed that Appellant had a computer that was turned on and that a word-processing document was showing on the screen. Detective Anderson informed Appellant that they were investigating the distribution of child pornography and running down some leads. When asked how long he had been living in Columbia, Appellant responded that he had been there for fourteen months but that he had stayed at his parent's house off and on during that period. Appellant indicated that he had an old computer still at his parent's house that he no longer used and that he had the computer in his apartment that he had previously

used at his parent's house. When asked what he used his computer for, Appellant stated that he used it for school work and to download music. Appellant admitted having file-sharing programs on his computer and that he had used them to download adult pornography before. Detective Anderson then asked Appellant whether he had ever downloaded child pornography, either on purpose or by accident. Appellant indicated that, on occasion, he had accidentally downloaded misnamed material that had turned out to be child pornography but that, once he realized what they were, he had deleted them. He further acknowledged that he had done so on his current computer while at his parent's home. Appellant admitted that it was possible that he may have failed to erase some of the child pornography that he had downloaded.

Detective Anderson asked Appellant for permission to examine his computer to verify that there was not active child pornography on it. Appellant denied Detective Anderson's request and asked to speak with his parents and the officers in St. Louis. Detective Anderson contacted the St. Louis County Sheriff's department and was told their officers would like to question Appellant at the Boone County Sheriff's Department. Detective Anderson conveyed that request to Appellant, and he agreed to meet with the officers from St. Louis at the Sheriff's Department.

Detective Anderson informed Appellant that he was going to apply for a search warrant to search the computer and told Appellant that Appellant should let him know up front if they were going to find child pornography on it. Appellant acknowledged that there would probably be child pornography files on the computer.

Detective Anderson then allowed Appellant to step outside to talk to his parents on the telephone. By that time, Detective Anderson had decided to seize the computer until a warrant could be obtained. Before unplugging the computer to take it, he decided to open and examine all of the programs currently running on the computer. From icons shown on the bottom, right corner of the computer screen, Detective Anderson could tell that several programs were running in addition to the word processing program shown on the screen. One of those programs was LimeWire, which Appellant had admitted having used to download music and videos.¹ When Detective Anderson clicked on that icon to open that program, he was able to see that

(footnotes omitted).

¹ This court described the nature of the LimeWire software in *State v. Tremaine*, 315 S.W.3d 769, 773 (Mo. App. W.D. 2010), noting:

LimeWire is a peer-to-peer ("P2P") computer application that allows users to trade computer files (generally audio and video files) over the Internet. LimeWire connects users to the Gnutella and Bit Torrent P2P networks, providing users access to files which other users choose to share over the networks. Users begin at LimeWire's website. There, they download to their computer the software necessary for file sharing by activating an installation "wizard" that walks the user through a step-by-step setup process. Once LimeWire is installed, the user can manually change default settings which are pre-set in the software to whatever particular settings the user wants for his or her computer.

To search for available files, LimeWire users enter a search term into a dialogue box, and the LimeWire network, in conjunction with Gnutella or similar software, assembles a list of files fitting the search terms which are available for download from other users' computers. The user then double clicks on a particular file to download it from another computer which is set to permit the sharing of such files. LimeWire assembles complete files for the requesting user by collecting pieces of the selected file, potentially collecting individual pieces from the computers of many different users which have the requested file. LimeWire verifies that it is accessing pieces of the correct file by means of a Secure Hash Algorithm (or "SHA 1") value which uniquely corresponds to an individual computer file. By default, pieces of computer files are initially downloaded into the "Incomplete" folder on the requesting user's computer; once a complete file is assembled, it is automatically transferred into another default folder called "Shared." However, LimeWire users determine whether the files in these folders are shared and actually available to other users. Thus, a user can select an option that precludes other users from downloading materials from his computer.

files were being downloaded and uploaded at that time. He took pictures of the screens showing lists of the filenames being uploaded and downloaded.

After seeing the names of the files being uploaded and downloaded on LimeWire, many of which had names suggesting they might contain child pornography, Detective Anderson told Appellant that files were being uploaded and downloaded on his computer. Appellant responded, "Yes, sir." Detective Anderson asked Appellant if he knew that he had child pornography on the computer. Appellant responded that he was aware that there would be child pornography on his computer but stated that he did not realize that he was sharing such material. When asked, Appellant indicated that the last time he had downloaded child pornography was the previous night and that he had used particular search terms to find such files. Appellant was then allowed to make some more telephone calls and then went with Detective Anderson to the Boone County Sheriff's Department to talk to the officers from St. Louis. Detective Anderson brought the computer with them. Once at the Sheriff's Department, Appellant changed his mind and indicated that he did not want to talk to the officers from St. Louis. Detective Anderson then gave him a ride back home.

The following day, Detective Anderson applied for a warrant to search Appellant's computer. In his affidavit in support of his warrant application, Detective Anderson relied, in part, on the information he discovered by examining the computer while at Appellant's apartment and comments made by Appellant after being confronted with that information. After the Circuit Court of Boone County granted that warrant, the hard drive on the computer was examined using forensic equipment and programs. That

examination revealed that numerous video files containing child pornography were present on Appellant's computer. The examination further revealed that LimeWire had been used to download such files, that those files had been made available for upload to others, and that such files had indeed been uploaded to others using LimeWire.

Appellant was charged in the Circuit Court of Boone County with one count of possession of child pornography and one count of second-degree promoting child pornography. Following a jury trial, Appellant was found guilty as charged and was sentenced to two concurrent terms of five years imprisonment.

In his sole point on appeal, Appellant claims that the trial court erred in denying his motion to suppress evidence obtained both directly and derivatively from Detective Anderson's warrantless search of his computer.² He argues that no recognized exception to the warrant requirement of the Fourth Amendment applies to the circumstances presented and, therefore, the search of his computer by Detective Anderson before a warrant was obtained violated his constitutional right to be free from unreasonable, warrantless search.

"When reviewing the trial court's overruling of a motion to suppress, we consider the evidence presented at both the suppression hearing and at trial to determine whether sufficient evidence exists in the record to support the trial court's ruling." *State*

² Appellant filed two motions to suppress. In one, he challenged the admission of the physical evidence taken from the computer. In the other, he challenged the admission of the statements he made to Detective Anderson. The trial court granted Appellant's motion related to his statements to Detective Anderson, excluding from evidence those statements made by Appellant after Detective Anderson clicked the LimeWire icon on Appellant's computer. The trial court denied Appellant's other motion, however, and allowed into evidence Detective Anderson's pictures and testimony related to his search of the active programs on the computer.

v. Loyd, 338 S.W.3d 863, 865 (Mo. App. W.D. 2011) (internal quotation omitted). "We reverse the trial court's decision only if it was clearly erroneous." *Id.* We defer to the trial court's credibility and factual determinations, *State v. Faruqi*, 344 S.W.3d 193, 199 (Mo. banc 2011), but we review *de novo* whether the Fourth Amendment was violated under the facts of the case. *Loyd*, 338 S.W.3d at 865.

"The Fourth Amendment to the United States Constitution guarantees that '[t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated." *Faruqi*, 344 S.W.3d at 204. "Article I, section 15 of the Missouri Constitution provides the same guarantees against unreasonable searches and seizures; thus, the same analysis applies to cases under the Missouri Constitution as under the United States Constitution." *State v. Oliver*, 293 S.W.3d 437, 442 (Mo. banc 2009).

"Generally, subject to certain exceptions, warrantless searches and seizures are deemed *per se* unreasonable." *Loyd*, 338 S.W.3d at 865. However, "[t]he state can overcome this presumption by demonstrating that the search or seizure falls within one of a carefully defined set of exceptions, many of which are based on the presence of exigent circumstances." *State v. Cromer*, 186 S.W.3d 333, 343-44 (Mo. App. W.D. 2005) (internal quotation omitted).

We begin our analysis by stating the obvious. When Detective Anderson began clicking on icons on Appellant's computer screen to view different programs that were

not openly visible on the computer screen, he was conducting a search.³ See United States v. Payton, 573 F.3d 859, 863 (9th Cir. 2009) (holding that an officer moving a mouse, deactivating a screen saver, and opening a file on a computer was a search requiring a warrant). For these purposes, using a mouse and/or keyboard to shuffle between files that are not plainly visible on an active computer screen is just as much of a search as opening and looking through Appellant's filing cabinets or desk drawers.⁴ In fact, "the nature of computers makes such searches so intrusive that affidavits seeking warrants for the search of computers often include a limiting search protocol, and judges issuing warrants may place conditions on the manner and extent of such searches to protect privacy and other important constitutional provisions." Id. at 864. Because "it is important to preserve the option of imposing such conditions when they are deemed warranted by judicial officers authorizing the search of computers," the generally accepted practice of law enforcement officers is "to stop and seek an explicit warrant when they encounter a computer that they have reasons to believe should be searched." Id.

³ Obviously, the on-site, physical search of a person's computer differs significantly from remotely accessing files on their computer through the use of peer-to-peer software that the person has installed to allow others remote access to those files. *See United States v. Stults*, 575 F.3d 834, 842-43 (8th Cir. 2009) (finding no 4th Amendment violation where the FBI remotely searched files made available by the defendant's installation and use of a file-sharing program that granted access to those files on his computer to anyone else that had the same file-sharing program).

⁴ See *Hoffa v. United States*, 385 U.S. 293, 301, 87 S.Ct. 408, 17 L.Ed.2d 374 (1966):

What the Fourth Amendment protects is the security a man relies upon when he places himself or his property within a constitutionally protected area, be it his home or his office, his hotel room or his automobile. There he is protected from unwarranted governmental intrusion. And when he puts something in his filing cabinet, in his desk drawer, or in his pocket, he has the right to know it will be secure from an unreasonable search or an unreasonable seizure.

Detective Anderson acknowledged that he was looking through the various programs running in the background on the computer in search of evidence. This was, in any sense of the term, a search.

Accordingly, we must next determine whether the trial court could have properly found that a recognized exception to the warrant requirement was applicable in this case. The State contends that the exigent circumstances justified the detective's actions in accessing the active programs because information in the computer's RAM (random access memory) would disappear when the officer unplugged the computer to seize it. In other words, the State argues that the "exigent circumstance" of the officer wanting to seize the computer, unplug it, and remove it from the apartment before obtaining a warrant justified his search of the active files on the computer.

"The justification for the exigency exception is time related, i.e., there is a need that will not brook the delay incident to obtaining a warrant." *Cromer*, 186 S.W.3d at 344 (internal quotation omitted). "Exigent circumstances exist if the time needed to obtain a warrant would endanger life, allow the suspect to escape, or risk the destruction of evidence." *Id.* (internal quotation omitted). "The subjective belief of the officer who conducted the [search] is not determinative. . . . [W]e look to the circumstances as they would have appeared to a prudent, cautious, and trained officer." *State v. Warren*, 304 S.W.3d 796, 801-02 (Mo. App. 2010).

The record in this case simply does not establish any pressing need for the officer to unplug the computer prior to obtaining a warrant. Three officers were present in the apartment and had fully secured the scene. The State failed to prove the

existence of exigent circumstances that would preclude an officer from remaining with the computer while a warrant was obtained. The State's argument in this regard is based entirely upon a presumption of inconvenience for the officers and Appellant's roommates. Such circumstances are simply not exigent and most certainly do not establish "a need that will not brook the delay incident to obtaining a warrant." *Id.* Though Detective Anderson's subjective belief is not the standard for determining exigent circumstances, if Detective Anderson truly believed that valuable evidence might be lost through the unplugging of the computer, he should have waited until a warrant was obtained and then conducted his search of the files active on the computer.⁵

The State also contends that exigent circumstances existed because Detective Anderson knew that files were actively being uploaded and downloaded and that this process might cease before a warrant could be obtained. In making this argument, the State mischaracterizes Detective Anderson's testimony that he was able to see that the LimeWire program was running from the visible computer screen as stating that he was aware that files were presently being uploaded and downloaded. Though Detective Anderson testified that, with LimeWire running, files of some type could possibly have been being actively uploaded or downloaded, he did not verify the fact that files were being actively shared until after he opened the LimeWire program. Moreover, the

⁵ We recognize that the officers were present in Appellant's apartment by consent and that this consent could have been withdrawn. The withdrawal of that consent, thereby requiring the officers to immediately remove the seized computer from the apartment, might well have given rise to sufficient exigency to justify Detective Anderson's actions, but we are not faced with that proposition in this case.

State's argument that the transfer of files of an unknown nature might be completed by the time a warrant was obtained is akin to saying that an officer couldn't wait for a wiretap warrant because the suspect was on the phone and might finish his conversation before a warrant could be obtained.

By searching Appellant's computer without a warrant, the State violated Appellant's right to be free from unlawful search and seizure. Ordinarily, "[e]vidence discovered and later found to be derivative of a Fourth Amendment violation must be excluded as fruit of the poisonous tree." *Oliver*, 293 S.W.3d at 442 (internal quotation omitted). Thus, any evidence uncovered derivative to Detective Anderson's unlawful search of the active computer files should have been excluded from evidence unless an exception to this rule applies.

The State alternatively argues on appeal that, regardless of whether Detective Anderson's actions in opening the active files on Appellant's computer violated the Fourth Amendment, the evidence was properly admitted at trial based upon the inevitable discovery doctrine. "[T]he inevitable discovery rule . . . provides that evidence obtained through unlawful means may be admissible if it can be shown that the same evidence would have been inevitably discovered in a lawful manner." *State v. Grayson*, 336 S.W.3d 138, 150 (Mo. banc 2011). "To show that the evidence would have inevitably been discovered, the state must prove by a preponderance of the evidence: (1) that certain standard, proper and predictable procedures inevitably would have led to discovery of the challenged evidence through the state's pursuit of a

substantial, alternative line of investigation at the time of the constitutional violation." *Oliver*, 293 S.W.3d at 443.

The State has failed to explain, nor do we perceive, how access to the active files on the computer to view and take pictures of the active programs was inevitable. Detective Anderson testified to his intent to turn off, unplug, and remove the computer from the premises prior to applying for a warrant. Thus, the record reflects that, as a result of Detective Anderson's own actions, the ability to view and photograph the active programs would not have existed by the time a warrant could be obtained for a lawful search to have been conducted. Admission of the pictures of the active computer screens or Detective Anderson's testimony related to his access of the active programs could not be justified by the inevitable discovery doctrine.⁶

To the extent that Appellant challenges the seizure of the computer's hard drive and the admission of the evidence ultimately recovered as result of a forensic examination of the hard drive after a search warrant was obtained, however, on the record before us, that evidence would clearly have been inevitably discovered. Detective Anderson informed Appellant of his intent to seize and to obtain a search warrant for the computer prior to his unlawful search and had more than sufficient probable cause to obtain a search warrant in light of Appellant's previous admission that he had downloaded child pornography and that some child pornography was likely still

⁶ Likewise, the statements made by Appellant after being confronted with that evidence was obtained as a direct result of the unlawful search and would not be admissible under the inevitable discovery rule. The trial court properly excluded those statements from evidence at trial, and they are not at issue in this case.

on his computer. While Appellant argues that this evidence should be viewed as fruit of the poisonous tree because Detective Anderson referenced the unlawfully obtained evidence in the affidavit in support of his application for the search warrant, "[t]he fact that illegally obtained evidence is included in the affidavit does not invalidate the warrant." *Id.* "The ultimate inquiry is not whether the affidavit contained allegations based upon illegally obtained evidence but whether, if setting aside all tainted allegations, the independent and lawful information stated in the affidavit suffices to show probable cause." *Id.* (internal quotation omitted). In this case, when the improperly obtained evidence is disregarded, the remaining evidence referenced in the affidavit more than sufficiently establishes probable cause for the issuance of the search warrant. The evidence recovered from the hard drive would have inevitably been discovered regardless of Detective Anderson's improper search of the active files on the computer, and the trial court did not err in admitting that evidence at trial.

In short, the trial court clearly erred in admitting the photographs and testimony related to the active files on Appellant's computer because that evidence was obtained during an improper, warrantless search by Detective Anderson in violation of Appellant's constitutional rights. The trial court did not, however, err in admitting the evidence ultimately uncovered through the forensic examination of Appellant's computer after a warrant was issued.

We must next consider whether the trial court's error requires reversal. "Constitutional errors . . . do not require reversal if the error was harmless beyond a reasonable doubt." *State v. Bynum*, 299 S.W.3d 52, 61 (Mo. App. E.D. 2009). "Harmless beyond a reasonable doubt means that no reasonable doubt exists that the admitted evidence failed to contribute to the jury's verdict." *State v. Brooks*, 304 S.W.3d 130, 137 (Mo. banc 2010).

In this case, the erroneously admitted photographs and testimony related to the active files on the computer were cumulative to evidence discovered during the forensic examination of Appellant's computer that was properly admitted into evidence. Though presented in a different format, evidence from the forensic examination of the computer and testimony related thereto reflected the same information contained in the improperly admitted photographs and testimony. The forensic evidence identified those files that were being actively uploaded from and downloaded to Appellant's computer while Detective Anderson was present in the apartment. "When evidence challenged on constitutional grounds is cumulative of other properly-admitted evidence, the disputed evidence could not have contributed to the defendant's conviction and is harmless beyond a reasonable doubt." *State v. Martin*, 291 S.W.3d 269, 288 (Mo. App. S.D. 2009).

Moreover, the properly admitted evidence of Appellant's guilt was overwhelming. Appellant admitted to the police having installed LimeWire on his computer and having used it to download videos. No evidence or argument was offered that someone else might have similarly used the computer. The forensic evidence clearly established that Appellant had downloaded and was in possession of the material charged in Count I on his computer and that he had offered for sharing through LimeWire the material charged in Count II. It was undisputed that this material was indeed child pornography, and the names of these files clearly and unmistakably reflect the nature of their content. In addition, the evidence from the forensic examination reflected the presence of at least 78 other child pornography videos on Appellant's computer, most of which similarly had file names indicative of their content. There appears no likelihood that exclusion of the pictures and testimony related to Detective Anderson's warrantless search of the active files on Appellant's computer could have affected the jury's verdict.

Since the erroneously admitted evidence was harmless beyond a reasonable doubt, Appellant's convictions and sentences are affirmed.

Joseph M. Ellis, Judge

All concur.