

FILED
Court of Appeals
Division II
State of Washington
9/17/2020 4:59 PM

FILED
SUPREME COURT
STATE OF WASHINGTON
9/18/2020
BY SUSAN L. CARLSON
CLERK

99045-0
No. 52544-5-II

IN THE COURT OF APPEALS, DIVISION II
OF THE STATE OF WASHINGTON

STATE OF WASHINGTON,

Respondent,

vs.

AARON MARK HARRIER,

Appellant.

PETITION FOR DISCRETIONARY REVIEW BY THE
WASHINGTON STATE SUPREME COURT

**APPELLANT'S PETITION FOR DISCRETIONARY REVIEW BY
SUPREME COURT**

BRIAN A. WALKER
Attorney for Appellant
Brian Walker Law Firm, P.C.
210 E. 22nd Street
Vancouver, WA 98663
brian@walkerlawfirm.com
(360) 695-8886

TABLE OF CONTENTS

Page

1. TABLE OF CONTENTS.....	i
2. TABLE OF AUTHORITIES.....	i
3. ISSUE PRESENTED.....	iii
4. STATEMENT OF THE CASE.....	1
5. ARGUMENT.....	4
6. CONCLUSION.....	18
7. APPENDIX.....	21
8. CERTIFICATE OF SERVICE	18

TABLE OF AUTHORITIES

Page

FEDERAL AND SUPREME COURT CASES

<i>Ex parte Jackson</i> , 96 U.S. 727.....	12
<i>Payton v. New York</i> , 445 U.S. 573, 586, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980).....	5
<i>U.S. v. Ackerman</i> , 831 F.3dn1292.....	13,14
<i>U.S. v. Jacobsen</i> , 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2d 85.....	8,9,10
<i>Walter v. United States</i> , 447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 410.....	10,12

Wong Sun v. United States, 371 U.S. 471, 83 S. Ct. 407, 9 L. Ed. 2d 441 (1963)5,6

STATE CASES

State v. Agee, 15 Wash.App. 709, 713-14, 552 P.2d 1084 (1976).....7

State v. Carter, 151 Wn.2d 118, 126-27, 85 P.3d 887 (2004)4,17,18

State v. Eisfeldt, 163 Wn.2d 628 (Wash. 2008), 185 P.3d 580.....4,5,15

State v. Harrier, 52544-5-II.....4

State v. Mannhalt, 33 Wash.App. 696, 702, 658 P.2d 15 (1983)..6,7

State v. McKee, 3 Wn.App.2d 11, 413 P.3d 1049, (Div. 1 2018)...7

State v. Reid, 98 Wn.App. 152, 988 P.2d. 1038 (1999).....5

State v. Samalia 186 Wn.2d 262, 375 P.3d 1082, (2016).....7

State v. Smith, 110 Wn.2d 658, 756 P.2d 722 (1988).....6

State v. Smith, 36 Wn.App. 133, 672 P.2d. 759 (1983).....10

State v. Trasvina, 16 Wn.App. 519, 557, 557 P.2d 368 (1976).....5

State v. Wolken, 103 Wn.2d 823, 700 P.2d 319, (1985)6

State v. Young, 123 Wn.2d 173, 180, 867 P.2d 593 (1994).....5

State v. Simpson, 95 Wn.2d 170, 178,622 P.2d 1199 (1980)5

CONSTITUTIONAL PROVISIONS

Fourth Amendment, U.S. Constitution.....4,6,14
Washington State Constitution article I, section 7
.....5,6,7,15

ISSUE AND ASSIGNMENT OF ERROR

Assignment of Error The Court erred by denying Defendant’s motion to suppress the depictions discovered in this case as a result of a warrantless search

Issue

Whether the warrantless search conducted by the investigating detective was illegal

¹STATEMENT OF THE CASE

(Unless otherwise indicated, the facts below are derived from CP 103, Pages 2-6)

On December 31, 2015, Synchronoss Technologies, a cloud-based storage provider for Verizon Wireless customers, automatically scanned Defendant's stored data and located six images with hash values presumably matching hash values of previously known ²child pornographic images. The scanning program Synchronoss used to scan the stored data, or whether it used a program at all, is unknown. How such program is designed, functions and is maintained is also unknown. Further, it is not known how the database of hash values, if any, used by Synchronoss for identifying known child pornographic images, was acquired, generated or maintained. The six images located by Synchronoss were not verified as being child pornographic images by a human being associated with Synchronoss.

¹The facts set forth in this Statement of the Case are derived chronologically from Findings of Fact and Conclusions of Law entered following a trial on stipulated facts, CP 103, pages 2-6. Therefore, Clerk's Papers citations will be limited to one at the top of the Statement and the only other citations will be to Clerk's Papers other than the narrative facts in CP 103.

²The term "child pornography" is used variously herein in place of Washington's term, "depictions of minors engaged in sexually explicit conduct", to be consistent with the wording on the "CyberTip" referred to in this Brief, and for brevity. No casual reference or rewording to the Washington State legal definition is intended.

Synchronoss provided to the National Center for Missing and Exploited Children (NCMEC), a ³CyberTip containing the six unopened electronic image files, as required by federal statute, together with the subscriber's (Defendant's) telephone number associated with the account from which the six images were seized by Synchronoss and forwarded to NCMEC. The CyberTip was automatically submitted on NCMEC's online form. Under "Incident Information" was the following information: "Incident Type: child pornography (possession, manufacture, and distribution)". CP 56, Exhibit 3, Page 8. There was no further information regarding the nature of the activity being reported in the CyberTip.

NCMEC also did not open or in any way view or compare the six image files. NCMEC only forwarded the CyberTip with the six unopened images to the Seattle regional law enforcement agency who then relayed the CyberTip together with the six yet unopened image files to Detective Jason Mills who is with the Vancouver Police Department (VPD) for follow up investigation.

Detective Mills opened and examined the six images without a warrant to visually confirm that the images appeared to be in fact depictions of children engaged in sexually explicit conduct.

³"CyberTip" is the term used by the federally created agency National Center for Missing and Exploited Children (NCMEC) for an online referral of activity involving suspected child pornography.

Detective Mills then wrote detailed descriptions of each image and incorporated the descriptions into his application for a search warrant to be served upon Synchronoss Technologies and Verizon Wireless. The search warrant was issued and directed Synchronoss and Verizon to provide information each company had which was associated with Defendant's account telephone number.

In response to the warrant, Synchronoss provided a thumb drive containing 10 more child pornographic images as well as Defendant's account information and a number of Defendant's personal family photos and a photo of a wallet displaying Defendant's Washington State Driver's License.

The Verizon response included information which associated the Defendant's name with the account telephone number.

Based upon the information obtained from Synchronoss and Verizon pursuant to the initial warrant, Detective Mills obtained another warrant for the Defendant's residence and served it on May 31, 2016. At the residence, Defendant's cellular telephone was seized, analyzed and determined to be the device that had been used to download and then upload the images to the Synchronoss cloud storage.

The Defendant was detained and interrogated. During questioning, Defendant admitted to viewing, and then downloading

to his cellular telephone the child pornographic images which had been discovered in his cloud-based storage as well as on his cellular telephone. There is no evidence that the Defendant had been aware that images on his cell phone were being uploaded to the cloud storage. The Defendant was arrested and charged with counts of Possession of Depictions of Minors Engaged in Sexually Explicit Conduct.

The Defendant was found guilty following a trial on stipulated facts and Division II of the Court of Appeals affirmed the conviction reasoning that, under *Eisfeldt*, there is no privacy interest in evidence provided to police by a private party and that, “additionally”, under *State v. Carter*, 151 Wn.2d 118, 126-27, 85 P.3d 887 (2004), “there is no privacy interest in contraband”. *State v. Harrier*, 52544-5-II, at Page 3.

ARGUMENT

The Court of Appeals erred by affirming the trial court’s denial of the Defendant’s motion to suppress evidence contained in electronic image files opened and examined by police without a warrant.

The Fourth Amendment of the U.S. Constitution protects citizens from unreasonable searches and seizures and requires that all warrants be issued "upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. Amend. IV. Warrantless searches and seizures inside a home are

presumptively unreasonable. *Payton v. New York*, 445 U.S. 573, 586, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980).

The Washington State Constitution Article I, Section 7, provides that “No person shall be disturbed in his private affairs, or his home invaded, without authority of law.” Washington State’s Constitution, Article I, Section 7, is explicitly broader than that of the Fourth Amendment as it “clearly recognizes an individual’s right to privacy with no express limitations” and places greater emphasis on privacy. *State v. Young*, 123 Wn.2d 173, 180, 867 P.2d 593 (1994) (quoting *State v. Simpson*, 95 Wn.2d 170, 178, 622 P.2d 1199 (1980)). Article I, Section 7 focuses on the privacy expectations of individuals rather than the “reasonableness” of a search. *State v. Eisfeldt*, 163 Wn.2d 628 (Wash. 2008), 185 P.3d 580.

In a motion to suppress evidence, a criminal defendant bears the initial burden of establishing that evidence was obtained unlawfully. *State v. Trasvina*, 16 Wn.App. 519, 557, 557 P.2d 368 (1976).

Once a prima facie case has been made that the search was illegal, the burden shifts to the State to establish that such evidence was obtained in a constitutionally sound manner. *State v. Reid*, 98 Wn.App. 152, 988 P.2d. 1038 (1999), *Wong Sun v. United States*, 371 U.S. 471, 83 S.Ct.407, 9 L.Ed.2d. 441 (1963). The burden is upon the State to show that the seizure of evidence was

constitutionally sound by clear and convincing evidence. *State v. Smith*, 36 Wn.App. 133, 672 P.2d. 759 (1983).

In the event that a search has been determined to be illegal, all that which has been obtained thereby is deemed inadmissible as evidence. *Wong Sun v. United States*, 371 U.S. 471, 487-88, 83 S. Ct. 407, 9 L. Ed. 2d 441 (1963) (evidence is inadmissible as the "fruit of the poisonous tree" where it has been obtained by illegal actions of the police). *State v. Smith*, 110 Wn.2d 658, 756 P.2d 722 (1988).

Acts by private citizens which are done at the behest of, or encouragement or requirement of the state, may render a private party an agent of the state for purposes of Article 1, Section 7 as well as the Fourth Amendment of the United States Constitution.

Because the exclusionary rule is inapplicable to the actions of private persons, the misconduct must be that of a government agent. It must be shown that the State in some way "instigated, encouraged, counseled, directed, or controlled" the conduct of the private person.

State v. Wolken, 103 Wn.2d 823, 700 P.2d 319, (1985), citing *State v. Mannhalt*, 33 Wash.App. 696, 702, 658 P.2d 15 (1983)

“Before the wrongful actions of a private citizen will be imputed to the State, it must be shown that the latter in some way instigated, encouraged, counseled, directed, or controlled the conduct in question.” *State v. Agee*, 15 Wash.App. 709, 713-14, 552 P.2d 1084 (1976), aff'd on other grounds, 89 Wash.2d 416, 573 P.2d 355 (1977). *State v. Mannhalt*, 33 Wn.App. 696, 658 P.2d 15, (Div. 1 1983).

As time and technology has advanced, so has the law has in its steady fashion, finding that individuals have a reasonable expectation of privacy in cell phones.

Given the intimate information that individuals may keep in cell phones and our prior case law protecting that information as a private affair, we hold that cell phones, including the data that they contain, are "private affairs" under article I, section 7. As private affairs, police may not search cell phones without first obtaining a warrant unless a valid exception to the warrant requirement applies.

State v. Samalia 186 Wn.2d 262, 375 P.3d 1082, (2016). See also *State v. McKee*, 3 Wn.App.2d 11, 413 P.3d 1049, (Div. 1 2018).

In this case, a police detective received six unopened files attached to a tip in an automated message from a company called

Synchronoss Technologies. The tip simply indicated, “Incident Type: Child Pornography (possession, manufacture, and distribution)”. The detective received no descriptions of the images, no information as to what Synchronoss Technologies is, and what, if any, verification had been performed regarding the six images. The detective then opened and viewed the six images without a warrant.

The State could argue that the detective merely repeated the search that a private individual had already done where a warrant would not be required. This argument fails, however, as among the other reasons set forth below, the detective’s search exceeded the scope of what Synchronoss was known to have done.

Though Appellant has found no Division II cases directly on point, there have been a number of instructive cases which are helpful in determining the direction of constitutional protection when private searches precede governmental searches.

In 1984, the U.S. Supreme Court found that a governmental search and field testing of an opened package of suspected cocaine delivered to law enforcement by Fed Ex employees was a constitutional search. *U.S. v. Jacobsen*, 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2d 85.

In *Jacobsen*, human being employees damaged a Fed Ex package with a forklift, opened the package to see if there was any

damage, for insurance purposes and pursuant to a company policy. Inside, they found a pipe, or “tube”, made from duct tape. The employees cut the tube open and discovered a white powdery substance in a clear bag located at the center of the pipe. An agent arrived and repeated the unpackaging and saw the white, powdery substance in the clear bag. The agent extracted enough of the white powdery substance to perform a field test and found it to be presumptively cocaine. The Court found that the result of the private, Fed Ex search put the agent ⁴lawfully in possession of the bag of white powder, without the need for a warrant. Ultimately, the Court noted that the field test that was conducted could only “reveal whether a substance is cocaine, and no other arguably ‘private ’fact”. *Jacobsen* at 124. In other words, even if the substance had turned out to be not cocaine, it would necessarily be merely some kind of white powder and nothing more — a fact which “reveals nothing of special interest”. *Id.*

Unlike *Jacobsen*, no person had looked at the six images in our case. To compare, had the Fed Ex employees been unjustifiably alarmed over a bag of what turned out to be, for example, talcum powder, there would be little offense to the privacy interests of the sender or recipient of the package. In our case, however, had the CyberTip been wrong, the images could have

⁴This holding has become to be known as the “private search doctrine”.

been only the innocent, private family photos that were among the items seized from the Defendant's cloud storage or other, possibly intimate and personal photos or videos, things that a private citizen would expect to remain private. It is this possibility that triggers the constitutional protection of a privacy interest in this case.

Jacobsen drew substantially for its reasoning from a 1980, U.S. Supreme Court case, *Walter v. United States*, 447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 410. In *Walter*, a box containing 871 ⁵illegal pornographic 8-millimeter films was inadvertently delivered to the wrong company by the name of "L'Eggs" Products, Inc., rather than its intended recipient, "Leggs", Inc.. Employees of L'Eggs opened the box and found the illicit films. Though unable to view the films as they were without a projector, the employees noted that suggestive drawings appeared on one side of the film container and a description of the illicit content of the films appeared on the other. Employees of L'Eggs called the FBI who's agents retrieved the box of films, observed the drawings and labeling just as the employees had, but then, without a warrant, went on to view a number of the films with a projector. The Supreme Court found the search performed by the police to be illegal.

⁵The films were homosexual pornography which, at the time, violated federal indecency laws.

[N]otwithstanding that the nature of the contents of these films was indicated by descriptive material on their individual containers, we are nevertheless persuaded that the unauthorized exhibition of the films constituted an unreasonable invasion of their owner's constitutionally protected interest in privacy. It was a search; there was no warrant; the owner had not consented; and there were no exigent circumstances. ...

To be sure, the labels on the film boxes gave them probable cause to believe that the films were obscene and that their shipment in interstate commerce had offended the federal criminal code. But the labels were not sufficient to support a conviction, Further investigation -- that is to say, a search of the contents of the films -- was necessary in order to obtain the evidence which was to be used at trial.

The fact that FBI agents were lawfully in possession of the boxes of film did not give them authority to search their contents. Ever since 1878, when Mr. Justice Field's opinion

for the Court in *Ex parte Jackson*, 96 U.S. 727, established that sealed packages in the mail cannot be opened without a warrant, it has been settled that an officer's authority to possess a package is distinct from his authority to examine its contents.

When the contents of the package are books or other materials arguably protected by the First Amendment, and when the basis for [sic] the seizure is disapproval of the message contained therein, it is especially important that this requirement be scrupulously observed.

Id at 655-7.

Though the present case does not involve a misdirected package, it does involve a fixed number of images which, as in *Walter*, were arguably protected by the First Amendment. The detective in our case leapt to opening and viewing the images based upon a computerized tip containing merely the conclusory statement, “child pornography, possession, manufacture, and distribution” — far less detail than the drawings and descriptions included in *Walter* which had been placed on the outside of the film containers by the owners themselves. It is also worth noting that the term “child pornography” is not a term used under Washington

State law which prefers the less ambiguous term “depictions of minors engaged in sexually explicit conduct”. There is actually no way to be sure that the term used in the CyberTip had the same meaning as required by Washington State law. We can only surmise that it was the word choice and judgment of a software writer or programmer.

In a 2016, 10th Circuit case perhaps more similar to the present one, *U.S. v. Ackerman*, 831 F.3d 1292, the warrantless opening of an email was deemed illegal in an opinion authored by now U.S. Supreme Court Justice Neil Gorsuch. In *Ackerman*, America Online (AOL) software discovered images attached to an email with hash values matching known contraband images. The known contraband images were ones which had been previously encountered and viewed in-house by trained, AOL employees who then catalogued the hash values into a database. However, when Ackerman’s images were discovered by the AOL software, no employee opened and verified that the suspect images, except for a single image, were in fact a true match to prior, known contraband images. AOL sent an automated CyberTip to NCMEC where an analyst who processed the CyberTip opened and described not just the one verified by AOL, but all four attached images. The search was deemed illegal as it exceeded the scope of the AOL search by opening the email and image files. There,

NCMEC was deemed a governmental agency and therefore, subject to the warrant requirement. The court found there that AOL had merely provided the unopened Image files in the attachment to NCMEC, but had not in fact opened the files. NCMEC's subsequent opening of the image files, the Court found, constituted an impermissible extension of the search done by AOL and was, therefore, an unlawful search.

In the present case, no assurances of reliability were present as in *Ackerman*, but the mere opening of the images constituted an impermissible expansion of the private search done by Synchross.

In all of the above cases, the searches by law enforcement were found to be illegal when determined to have exceeded the scope of the search performed independently and prior by private individuals or companies. Further, the report of the suspected illegal activity was referred to law enforcement in most cases by human beings who had acted on their own who and could report their own observations. Moreover, in all of the cases, except the present one, it was established that a human being had either viewed the suspected contraband during the private search occurred.

The foregoing Fourth Amendment analysis notwithstanding, the Washington State Constitution does not make room for the private search doctrine. In 2008, the Washington State Supreme

Court issued its opinion in *State v. Eisfeldt* stating a rejection of the private search doctrine under the Washington State Constitution.

State v. Eisfeldt, 163 Wn.2d 628 (Wash. 2008), 185 P.3d 580.

In *Eisfeldt*, police were called to a private residence by a repairman who had been hired by the homeowner and given free access to the home. The repairman found what he believed to be evidence of a marijuana grow operation, called police and allowed them to enter and search the home. After being charged with the crime of manufacturing a controlled substance, Eisfeldt moved to suppress evidence found as a result of unlawful search which motion was denied. He was found guilty following a trial on stipulated facts and the court of appeals upheld the trial court's verdict. On review, the Washington State Supreme Court overturned the conviction finding, among other grounds, that the private search doctrine is not recognized under Article 1, Section 7 of the Washington State Constitution.

In our case, the Court of Appeals analysis is not supported by the law. First, the "private search" and delivery to law-enforcement of the electronica files in our case are in no way equivalent to the private actions that are set forth in *Eisfeldt*. There, the private citizen repairman, acting on his own suspicions, invited law enforcement in a location they had no right to be. A critical distinction, however, is that the repairman, was under no obligation

to report what he observed to police, but chose to do so on his own. The form of private search acknowledged as constitutional in the footnotes (9) in *Eisfeldt* refers to the actions of a private party acting on their own and with no lawful obligation to report the activity to police. That is not what occurred in our case.

In our case, even though Synchronoss' "search" of the Defendant's cloud storage may not have been illegal or required, once it found what corresponded to "child pornography", it was required to deliver the evidence to law-enforcement. The Court of Appeals acknowledges this in its opinion saying, that it did so as it was ⁶"legally required". As such, the "private actor" in our case was acting pursuant to a governmental requirement and therefore was acting as a government agent for this purpose.

Notwithstanding the propriety of the initial search and mandatory delivery to law-enforcement, at the time the electronic files had made their way into the hands of the detective in this case, not a single individual had identified or confirmed the contents of the electronic files and the detective had no way of knowing what he would observe unless and until he opened the files. Moreover, since the only other governmental agency which had been involved was NCMEC, which had not taking any measures to confirm the

⁶ Even though the Court of Appeals has ordered publication of *Harrier*, it has not been formatted to accommodate a proper citation as of the writing of this brief.

contents of electronic files, and since the detective had no knowledge of Synchronoss, its function, method of operation or reliability, he could place no reliance on the representation set forth in the Cyber Tip.

Additionally, there was no emergency, and no exigent or other circumstances, which excused the detective's decision to not seek a warrant. The true intrusion into the Defendant's private affairs, and the need for a warrant, is also borne out by the fact that the database obtained by law-enforcement from Synchronoss included personal, innocent family photos as well as other personal documents.

Second, the Court of Appeals' reasoning that the Defendant could have no privacy interest in the "contraband" seized in this case under, *State v. Carter*, is misplaced. In *Carter*, investigators observed an illegally modified AR-15 rifle which had been intentionally placed in public view by the defendant. One of the investigators noted by looking at the rifle that the safety lever had been rotated to the automatic firing position, rendering the AR-15 a fully automatic machine gun, which could only be accomplished through modification. As it is illegal for a citizen to possess a machine gun, the firearm was clearly an illegal item to possess.

In our case, the electronic files could not have been known to be illegal contraband by the investigating officer without actually

searching the files. Otherwise, he would not have had to open and view them. The files were only delivered with basically a label and what could be characterized as a note from an unknown person of what they contained. The Court of Appeals' comparison our case to *Carter* might have been appropriate had the Defendant knowingly displayed to the public child pornography which could be readily identified as such by an ordinary observer. That is not the case here, therefore, this logic does not address the Defendant's expectation of privacy in the objects seized by Synchronoss and the search without a warrant by law-enforcement.

The fact that the detective may have been lawfully in possession of the let electronic files did not give him authority to search their contents.

Since a search of the images was illegal, any evidence obtained as a result thereof, including the evidence set forth in the detective's affidavit, was fruit of the poisonous tree. Therefore, the image descriptions he made of the images themselves and should have been suppressed. Further, since the detective used the illegally obtained evidence to obtain subsequent search warrants, any such evidence should be suppressed as well as fruit of the poisonous tree.

CONCLUSION

Police performed a warrantless search of six images provided by an unknown private party who indicated that the images were suspected contraband images. The private party did not open or view the images or describe them. The police search exceeded the private search which occurred prior and therefore a warrant was required. All evidence in this matter was obtained as fruit of the poisonous tree and should be suppressed.

DATED this _____ day of September, 2020.

Respectfully Submitted:

BRIAN A. WALKER, WSBA # 27391
Attorney for Defendant Harrier

APPENDIX

June 23, 2020

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON

DIVISION II

STATE OF WASHINGTON,

Respondent,

v.

AARON MARK HARRIER,

Appellant.

No. 52544-5-II

UNPUBLISHED OPINION

SUTTON, J. — Aaron Mark Harrier appeals his convictions for two counts of first degree possession of depictions of a minor engaged in sexually explicit conduct and for three counts of second degree possession of depictions of a minor engaged in sexually explicit conduct. An internet cloud storage service provider, Synchronoss Technologies, Inc., ran a cursory search of all stored digital files and found six digital images with hash values matching those of known instances of child pornography. Synchronoss reported this information via CyberTip to the National Center for Missing and Exploited Children (NCMEC) who forwarded the information to local police for investigation.

Harrier argues that the police, by opening and viewing the images from NCMEC, exceeded the scope of Synchronoss' lawful search of the images and thus, the opening and viewing of the images was unlawful, and the trial court erred by denying his motion to suppress. Harrier relies on the Fourth Amendment to the United States Constitution and argues that the police's opening of the files was an expansion of the lawful search. Whether the police expanded a lawful search

is a factor that is considered under the private search doctrine, but the private search doctrine is applicable under the Fourth Amendment. Because Article 1, section 7 of the Washington Constitution is more narrow than the Fourth Amendment, we resolve this matter under our state constitution.

We hold that Harrier has no privacy interest in the images obtained by Synchronoss and delivered to the police. Therefore, the police's opening and viewing of the digital images was not an unlawful search. Thus, the trial court did not err by denying Harrier's motion to suppress. Accordingly, we affirm Harrier's convictions.

FACTS

Synchronoss provides cloud based storage for Verizon Wireless customers.¹ At all times material to this case, Harrier had a Verizon account and subscribed to Synchronoss cloud storage. In 2015, Synchronoss conducted a search of its subscriber cloud database using the "hashing" technique.² As a result of this search, Synchronoss discovered six digital images associated with Harrier's Verizon account. These images had identical hash values to those identified in prior

¹ See *United States v. Crawford*, ___ F. Supp. 2d ___, 2019 WL 3207854, slip op. at 2 (N.D. Oh. 2019).

² "[A] hash value is 'an algorithmic calculation that yields an alphanumeric value for a file.'" *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018) (quoting *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013)). "[A] hash value is a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file's contents." *Reddick*, 900 F.3d at 637. "Hash values are regularly used to compare the contents of two files against each other. 'If two nonidentical files are inputted into the hash program, the computer will output different results. If the two identical files are inputted, however, the hash function will generate identical output.'" *Reddick*, 900 F.3d at 637 (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 541 (2005)).

No. 52544-5-II

law enforcement investigations as being child pornography. As required under federal law,³ Synchronoss submitted an online CyberTip of “[c]hild [p]ornography (possession, manufacture, and distribution)” to NCMEC. Clerk’s Papers (CP) at 100.

NCMEC did not open or view the six images. Rather, NCMEC forwarded the CyberTip, including digital files of the images, to the Vancouver Police Department who assigned Detective Jason Mills to investigate.

Detective Mills opened and viewed the six image files to confirm that the images were child pornography. Based on his training and experience, he determined that the six images consisted of nude and partially nude prepubescent female children engaged in the lewd and lascivious display of their genitalia. Detective Mills then obtained search warrants based on the descriptions of the images and served them on Verizon and Synchronoss. The search warrant directed Synchronoss to provide “all information” held by Synchronoss associated with the suspect telephone number associated with the images. CP at 106.

Detective Mills received information from Verizon that confirmed that Harrier was the subscriber/account holder for the suspect telephone number. Synchronoss provided Detective Mills with a thumb drive containing account data associated with the suspect telephone number. The account data consisted of files containing family pictures of Harrier, including a photograph of a wallet displaying Harrier’s Washington State Driver’s License. The thumb drive also contained additional images depicting minors engaged in sexually explicit conduct. Detective

³ 18 U.S.C. § 2258A.

No. 52544-5-II

Mills reviewed these images. At least 10 of the images depicted nude or partially nude, prepubescent children engaged in sexually explicit activities with adults.

Based on a detailed description of the images, Detective Mills then obtained a search warrant for Harrier's residence. When executing the search warrant, Detective Mills seized Harrier's cell phone. The cell phone was determined to be the same phone associated with the Verizon account and the Synchronoss files that were the basis of the initial search warrant.

Law enforcement interviewed Harrier after advising him of his constitutional rights⁴ prior to asking questions. Harrier admitted to law enforcement that he had viewed images of minors engaged in sexually explicit conduct and that he had downloaded and/or saved images depicting minors engaged in sexually explicit conduct. Harrier also stated he used his cell phone for this purpose.

The State charged Harrier with two counts of first degree possession of depictions of a minor engaged in sexually explicit conduct and three counts of second degree possession of depictions of a minor engaged in sexually explicit conduct. Prior to trial, Harrier filed a motion to suppress the evidence against him, and the trial court denied the motion following a CrR 3.6 hearing.

The parties proceeded to a stipulated facts bench trial. The trial court found Harrier guilty as charged. Harrier appeals his convictions.

⁴ *Miranda v. Arizona*, 384 U.S. 436, 444, 86 S. Ct. 1602, 16 L. Ed. 2d 694 (1966).

ANALYSIS

Harrier argues that Detective Mills, by opening and viewing the images sent by NCMEC, exceeded the scope of Synchronoss' lawful private search of the images and that the opening and viewing of the images was unlawful. Harrier bases his argument on the Fourth Amendment to the United States Constitution. But the expansion of the private search doctrine is applicable under the Fourth Amendment, and is inapplicable under Article 1, section 7 of the Washington Constitution. As discussed below, we resolve this matter under our state constitution.

We hold that Harrier has no privacy interest in the images obtained by Synchronoss and delivered to the police; therefore, the police's viewing of the images was not a warrantless search. Accordingly, the trial court did not err by denying Harrier's motion to suppress and we affirm Harrier's convictions.

"[W]arrantless searches and seizures are per se unreasonable, in violation of the Fourth Amendment to the United States Constitution and article I, section 7 of the Washington Constitution." *State v. Garvin*, 166 Wn.2d 242, 249, 207 P.3d 1266 (2009). The Fourth Amendment protects a person's subjective and reasonable expectation of privacy. *State v. Hinton*, 179 Wn.2d 862, 868, 319 P.3d 9 (2014). And article I, section 7 provides that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law." WASH. CONST. art. 1, § 7. However, "[i]f a private affair is not disturbed, then there is no violation of article I, section 7." *State v. Reeder*, 184 Wn.2d 805, 814, 365 P.3d 1243 (2015). A defendant has the burden of proving a disturbance of his private affairs under article I, section 7. *State v. Butler*, 2 Wn. App. 2d 549, 557, 411 P.3d 393 (2018).

“[H]ash value comparison ‘allows law enforcement to identify child pornography with almost absolute certainty,’ since hash values are ‘specific to the makeup of a particular image’s data.’” *Reddick*, 900 F.3d at 639 (quoting *United States v. Larman*, 547 F. App’x 475, 477 (5th Cir. 2013) (unpublished)). Tips to NCMEC from service providers and from NCMEC itself are considered to be from “reliable sources.” *Millette v. U.S.*, ___ F. Supp. 2d ___, slip op. at 6, 2018 WL 3478891 (D. Me. 2018).

Under the private search doctrine, a warrantless search by a state actor that does not expand the scope of the private search does not offend the Fourth Amendment. *State v. Eisfeldt*, 163 Wn.2d 628, 636, 185 P.3d 580 (2008). The private search doctrine was established in *Walter v. United States*, 447 U.S. 649, 100 S. Ct. 2395, 65 L. Ed. 2d 410 (1980), and later applied in *United States v. Jacobsen*, 466 U.S. 109, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984) to sanction a warrantless search by state actors. The private search doctrine is based on the rationale that an individual’s reasonable expectation of privacy is destroyed when the private actor conducts his search. *Jacobsen*, 466 U.S. at 119.

Our Supreme Court held in *Eisfeldt* that the private search doctrine is inapplicable under our State Constitution. The court in *Eisfeldt* also recognized that when a private party hands evidence over to the police, there is no privacy interest in that evidence. 163 Wn.2d at 638 n.9. Additionally, there is no privacy interest in contraband. *State v. Carter*, 151 Wn.2d 118, 126-27, 85 P.3d 887 (2004). And child pornography is contraband. *State v. Garbaccio*, 151 Wn. App. 716, 729, 214 P.3d 168 (2009).

Here, it is undisputed that Synchronoss, a private party, conducted the initial lawful search using the “hashing” technique. The hash value of images from Harrier’s cell phone was identical

No. 52544-5-II

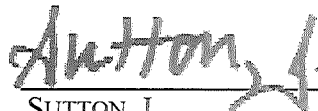
to the hash value of images previously identified as child pornography by law enforcement. It is also undisputed that Synchronoss then made a legally required CyberTip to NCMEC, who forwarded the information and tip to the police for investigation.

We know from the hash values that the files Synchronoss found were child pornography and that this information, the images, and the CyberTip are reliable. *See Millette v. U.S.*, ___ F. Supp. 2d ___, slip op. at 6, 2018 WL 3478891 (D. Me. 2018). Because a private party conducted the search and the images are contraband, Harrier did not have a privacy interest in them. Thus the police's opening and viewing the images from a private party was not unlawful. *See Carter*, 151 Wn.2d at 126-27. Accordingly, Harrier's arguments fail.

CONCLUSION

We hold that the trial court did not err by denying Harrier's motion to suppress. Accordingly, we affirm Harrier's convictions.

A majority of the panel having determined that this opinion will not be printed in the Washington Appellate Reports, but will be filed for public record in accordance with RCW 2.06.040, it is so ordered.



SUTTON, J.

We concur:



LEE, C.J.



WORSWICK, J.

2016

FILED

JUN 15 2018

2:30 PM
Scott G. Weber, Clerk, Clark Co.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF CLARK

STATE OF WASHINGTON,
Plaintiff,
v.
AARON HARRIER,
Defendant.

No. 16-1-01186-1

STIPULATED FACTS ON
NON-JURY TRIAL

COME NOW Plaintiff State of Washington appearing by and through Jeff McCarty, Deputy Prosecuting Attorney for Clark County, and Defendant Aaron Harrier, in person and with his attorney Brian Walker, Defendant having previously entered a knowing, intelligent and voluntary written waiver of his right to trial by a jury, and of his right to hear and confront witnesses against him and of his right to call witnesses on his own behalf and to compel their attendance, and the Defendant and the Plaintiff stipulate to the following undisputed facts:

1. On December 31, 2015, Synchronoss Technologies, an Internet Service Provider (ISP) of cloud base storage for Verizon Wireless, automatically scanned its subscriber

1 cloud database and discovered six images with hash values matching ones on a list of
2 such hash values previously identified as being suspected child pornography. It is not
3 known how the list of hash values was generated or maintained. It is not known how
4 the scanning program operates to conduct its scan. The discovery and characterization
5 of the six images were not verified by a human being. Synchronoss submitted a
6 cybertip to the National Center for Missing and Exploited Children (NCMEC). As an
7 ISP, Synchronoss was required by federal statute to forward the above described
8 cybertip to NCMEC. The cybertip indicated that Synchronoss had found what they
9 identified as six images suspected to be of minors engaged in sexually explicit conduct.
10 The images had been uploaded to their servers on December 31, 2015 and were
11 associated with a Verizon telephone number (360-949-0630) that was associated to
12 Aaron Harrier in Vancouver, Washington. NCMEC did not open or view the six images
13 in any way. NCMEC forwarded the cybertip, including digital files of the six images, to
14 law enforcement. The cybertip ultimately ended up with Detective Jason Mills of the
15 Vancouver Police Department.
16
17

18
19 2. Detective Mills opened and examined the digital files. Detective Mills opened
20 and viewed the six image files without a warrant. Detective Mills, based upon his
21 training and experience, determined that the images consisted of nude and partially
22 nude prepubescent female children engaged in the lewd and lascivious display of their
23 genitalia. Descriptions of some of the images are as follows:
24

- 25 • This image depicts a nude, prepubescent female who appears to be
26 under the age of eight (8). The child is lying on her stomach on pink
27

1 and white blankets facing away from the camera and her pelvis and
2 buttocks are raised. The child's legs are spread apart, creating lewd
3 and lascivious display of her anus and vagina. The child's vagina
4 lacks signs of maturation as there is no presence of pubic hair or
5 darkening of the skin surrounding the labia.

- 6
- 7 • This image depicts a nude, prepubescent female under the age of 10
8 (10). The child is lying on a bed with what appear to be adult females,
9 one of them nude, on both sides of her. The child's legs are spread
10 apart creating lewd and lascivious display of her vagina and anus. The
11 child's vagina lacks signs of maturation as there is no sign of pubic hair
12 or darkening of the skin surrounding the labia. The nude apparent
13 female adult female on the right side of the image is touching the
14 child's vaginal region.
- 15
- 16
- 17 • This image depicts two (2) nude, prepubescent females who appear to
18 be under the age of ten (10). The child in the forefront of the image is
19 lying back in between the legs of the child in the background with her
20 arm draped over the child's leg creating a lewd and lascivious display
21 of her undeveloped breasts. The child's legs in the forefront of the
22 image are spread apart creating lewd and lascivious display of her
23 vagina and anus. The child's vagina lacks signs of maturation as there
24 is no presence of pubic hair or significant darkening of the skin
25 surrounding the labia.
- 26
- 27

- This image depicts a nude, prepubescent female who appears to be under the age of ten (10). The child is sitting back on a tan sofa with both arms raised up and back behind her head so as to create a lewd and lascivious display of her undeveloped breasts. The child's legs are slightly spread apart offering lewd and lascivious display of her vagina. The child's vagina lacks signs of maturation with no presence of pubic hair growth or darkening of the skin surrounding the labia.

3. In February of 2016, Detective Mills obtained search warrants and served them upon Verizon Wireless and Synchronoss Technologies. The warrant itself directed Synchronoss to provide "all information" held by Synchronoss associated with the suspect telephone number. Detective Mills received information from Verizon that confirmed that the defendant, Aaron Harrier, was the subscriber/account holder for 360-949-0630. Synchronoss provided Detective Mills with a thumb drive containing account data associated with the telephone number 360-949-0630. The thumb drive contained files containing and family pictures of the defendant, including a photograph of a wallet displaying the defendant's Washington State Driver's License.

4. The thumb drive from Synchronoss also contained additional images of depictions of minors engaged in sexually explicit conduct. Detective Mills reviewed these images. At least ten (10) of the images depicted nude or partially nude, prepubescent children engaged in penile-vaginal intercourse, oral intercourse, or digital intercourse with adults. Descriptions of some of the images are as follows:

- This image depicts a nude, prepubescent female under the age of 10

BASED UPON THE DESCRIPTIONS PROVIDED IN # 2 ABOVE.

Q



1 (10) engaged in penile-vaginal intercourse with an adult male. The
2 child's legs are spread apart as she is sitting on the adult male who is
3 lying supine on a bed. The adult male is supporting the child with his
4 legs and hand while guiding his penis into the child's vagina.

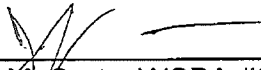
- 5 • This image depicts a nude, prepubescent female under the age of
6 eight (8) lying supine on a bed. The child is unclothed from the waist
7 down and her shirt is partially raised. The child's legs are spread apart
8 and what appears to be an adult female is engaged in oral sex with the
9 child's vagina.
10
11


12 5. Vancouver Police obtained a search warrant for the residence of the defendant,
13 Aaron Harrier. The warrant was served on May 31, 2016. The residence is located in
14 Clark County, Washington. Police contacted the defendant at that time and seized the
15 defendant's cell phone. The phone was determined to be the same phone associated
16 with the Verizon account and Synchronoss files that were the basis of the search
17 warrant.
18


19 6. The Defendant was interviewed by law enforcement. The defendant was
20 advised of his Constitutional rights prior to answering questions. The defendant
21 admitted to law enforcement that he had viewed images of minors engaged in sexually
22 explicit conduct and that he had downloaded and/or saved images depicting minors
23 engaged in sexually explicit conduct. The defendant also stated he used his phone for
24 this purpose and no other internet access within the confines of his home other than the
25 cell phone.
26
27

1 7. The defendant was physically located in Clark County, WA when he viewed and
2 possessed the above referenced images.
3

4 DATED this 15 day of June, 2018.
5

6 
7 _____
8 Jeff McCarty, WSBA #33134
9 Deputy Prosecuting Attorney
10 Attorney for Plaintiff

6 
7 _____
8 Brian Walker, WSBA #27391
9 Attorney for Defendant

10 
11 _____
12 Aaron Harrier
13 Defendant
14
15
16
17
18
19
20
21
22
23
24
25
26
27

CERTIFICATE OF SERVICE


I certify that on September 17, 2020, I provided a copy of the Appellant's Opening Brief by first class mail on the below-named, by mailing to said individuals copies thereof, contained in sealed envelopes, with postage prepaid, addressed to said individuals at said individuals 'last known addresses as set forth below, and deposited in the post office at Vancouver, Washington on said day.

By way of United States Postal Service, First Class Mail to the Following:

RACHEL ROGERS, ATTORNEY FOR RESPONDENT
CLARK COUNTY PROSECUTING ATTORNEY
PO BOX 5000
VANCOUVER, WA 98666

AARON HARRIER
11328 NE 51ST CIRCLE # P150
VANCOUVER, WA 98682

Dated this 17 day of September, 2020.



YESENIA PIEDRA
Legal Assistant

BRIAN WALKER LAW FIRM, P.C.

September 17, 2020 - 4:59 PM

Transmittal Information

Filed with Court: Court of Appeals Division II
Appellate Court Case Number: 52544-5
Appellate Court Case Title: State of Washington, Respondent v. Aaron Mark Harrier, Appellant
Superior Court Case Number: 16-1-01186-1

The following documents have been uploaded:

- 525445_Petition_for_Review_20200917165749D2306169_4149.pdf
This File Contains:
Petition for Review
The Original File Name was STATEMENT OF THE CASE 9-17-20.pdf

A copy of the uploaded files will be sent to:

- CntyPA.GeneralDelivery@clark.wa.gov
- aaron.bartlett@clark.wa.gov

Comments:

Sender Name: Faith Cagle - Email: faith@brianwalkerlawfirm.com

Filing on Behalf of: Brian A Walker - Email: brian@brianwalkerlawfirm.com (Alternate Email: yesenia@brianwalkerlawfirm.com)

Address:
210 E 22nd Street
Vancouver, WA, 98663
Phone: (360) 695-8886

Note: The Filing Id is 20200917165749D2306169