

FILED
Court of Appeals
Division III
State of Washington
9/24/2018 10:58 AM

FILED
SUPREME COURT
STATE OF WASHINGTON
10/3/2018
BY SUSAN L. CARLSON
CLERK

96380-1

Supreme Court No. (to be set)
Court of Appeals No. 35099-1-III
IN THE SUPREME COURT
OF THE STATE OF WASHINGTON

STATE OF WASHINGTON,
Respondent,
vs.

Jay Friedrich
Appellant/Petitioner

Walla Walla County Superior Court Cause No. 16-1-00228-2
The Honorable Judge John W. Lohrmann

PETITION FOR REVIEW

Manek R. Mistry
Jodi R. Backlund
Attorneys for Appellant/Petitioner

BACKLUND & MISTRY
P.O. Box 6490
Olympia, WA 98507
(360) 339-4870
backlundmistry@gmail.com

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF AUTHORITIES iii

INTRODUCTION..... 1

DECISION BELOW AND ISSUES PRESENTED 1

STATEMENT OF THE CASE..... 2

ARGUMENT WHY REVIEW SHOULD BE ACCEPTED..... 4

I. The Supreme Court should accept review to resolve an inconsistency in the standard for reviewing a magistrate’s decision to issue a search warrant. 4

II. The Supreme Court should accept review to determine how courts should assess staleness in cases involving search warrants for digital images. 5

A. Authorization to search a private residence may not rest on stale information..... 6

B. The warrant to search the Jensen residence rested on stale information..... 7

III. The Supreme Court should accept review and reverse because the warrant application rested primarily on broad generalizations about the common habits of “child pornography collectors.” 10

IV. The Supreme Court should accept review and reverse because the warrant was overbroad. 12

A. A warrant to search a private residence must be based on probable cause and must describe with scrupulous exactitude any items presumptively protected by the First Amendment. 13

B. The warrant application did not supply probable cause for numerous items listed in the warrant, including material protected by the First Amendment..... 15

C. The warrant failed to particularly describe most of the material subject to seizure, including items protected by the First Amendment.
17

D. The Court of Appeals misapplied the severability doctrine. 20

CONCLUSION 22

Appendix: Court of Appeals Decision

TABLE OF AUTHORITIES

FEDERAL CASES

<i>Hamer v. Neighborhood Hous. Servs. of Chicago</i> , --- U.S. ---, 138 S. Ct. 13, 199 L. Ed. 2d 249 (2017).....	20
<i>Stanford v. Texas</i> , 379 U.S. 476, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965)..	14, 15
<i>Steagald v. United States</i> , 451 U.S. 204, 101 S. Ct. 1642, 68 L. Ed. 2d 38 (1981).....	13
<i>United States v. Burkhart</i> , 602 F.3d 1202 (10th Cir. 2010).....	12
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010).....	20
<i>United States v. Lacy</i> , 119 F.3d 742 (9th Cir.1997)	12
<i>United States v. Riccardi</i> , 405 F.3d 852 (10th Cir. 2005)	12
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978).....	14

WASHINGTON STATE CASES

<i>State v. Chamberlin</i> , 161 Wn.2d 30, 162 P.3d 389 (2007).....	4
<i>State v. Chenoweth</i> , 160 Wn.2d 454, 158 P.3d 595 (2007)	4
<i>State v. Garbaccio</i> , 151 Wn. App. 716, 214 P.3d 168 (2009).....	12
<i>State v. Garcia-Salgado</i> , 170 Wn.2d 176, 240 P.3d 153 (2010)	4
<i>State v. Griffith</i> , 129 Wn.App. 482, 120 P.3d 610 (2005)	16, 17, 21
<i>State v. Gunwall</i> , 106 Wn.2d 54, 720 P.2d 808 (1986)	6
<i>State v. Higgs</i> , 177 Wn. App. 414, 311 P.3d 1266 (2013), <i>as amended</i> (Nov. 5, 2013).....	14
<i>State v. Jackson</i> , 150 Wn.2d 251, 76 P.3d 217 (2003)	4, 5

<i>State v. Keodara</i> , 191 Wn. App. 305, 364 P.3d 777 (2015), <i>review denied</i> , 185 Wn.2d 1028, 377 P.3d 718 (2016).....	11
<i>State v. Ladson</i> , 138 Wn.2d 343, 979 P.2d 833 (1999)	12
<i>State v. Lyons</i> , 174 Wn.2d 354, 275 P.3d 314 (2012).....	4, 6, 7, 8, 9, 10
<i>State v. Maddox</i> , 152 Wn.2d 499, 98 P.3d 1199 (2004).....	4, 11
<i>State v. McKinney</i> , 148 Wn.2d 20, 60 P.3d 46 (2002).....	12, 19
<i>State v. Meneese</i> , 174 Wn.2d 937, 282 P.3d 83 (2012)	6
<i>State v. Neth</i> , 165 Wn.2d 177, 196 P.3d 658 (2008).....	4
<i>State v. Ollivier</i> , 178 Wn.2d 813, 312 P.3d 1 (2013).....	4
<i>State v. Perrone</i> , 119 Wn.2d 538, 834 P.2d 611 (1992)..	14, 15, 16, 17, 18, 20, 22
<i>State v. Snapp</i> , 174 Wn.2d 177, 275 P.3d 289 (2012)	12, 19
<i>State v. Thein</i> , 138 Wn.2d 133, 977 P.2d 582 (1999).....	11
<i>State v. White</i> , 135 Wn.2d 761, 958 P.2d 962 (1998).....	6
<i>Town of Woodway v. Snohomish Cty.</i> , 180 Wn.2d 165, 322 P.3d 1219 (2014).....	5

CONSTITUTIONAL PROVISIONS

U.S. Const. Amend. I.....	13, 14, 15, 17, 18, 21, 22
U.S. Const. Amend. IV	3, 6, 11, 12, 13, 18, 19
Wash. Const. art. I, §7.....	3, 6, 11, 12, 18, 19

OTHER AUTHORITIES

18 U.S.C. §2258A.....	8, 9
RAP 13.4.....	5, 10, 13, 17, 20, 22

INTRODUCTION

Based on a single upload of a digital image, police obtained a warrant to search a residence for records, documents, and other non-digital media that “pertain[ed] to” or “relate[d] to” child pornography, as well as books and magazines that contained illegal images. The warrant also authorized police to seize all electronic devices and digital media, to enable a search for any “data that is capable of being read or interpreted by a computer,” even if the items and the data did not relate to child pornography. The search warrant amounted to a general warrant that permitted police to rummage through a household’s private papers and electronic media, and granted police unfettered discretion to decide which materials to seize. The evidence should have been suppressed.

DECISION BELOW AND ISSUES PRESENTED

Petitioner/appellant Jay Friedrich asks the Court to review the Court of Appeals Published Opinion (OP).¹ This case presents six related issues:

1. What does it mean to review a probable cause determination “de novo” while also giving “great deference” to the magistrate who issued a search warrant?
2. Is a warrant unsupported by probable cause when the supporting affidavit fails to provide facts allowing a magistrate to determine if allegations of criminal activity are stale?
3. Under the state constitution, must a magistrate assessing probable cause disregard the affiant’s generalizations regarding common habits of criminals?

¹ A copy of the opinion, entered August 23, 2018, is attached.

4. Was the warrant in this case overbroad because it authorized police to search for and seize numerous items for which the affidavit failed to supply probable cause?
5. Was the warrant in this case overbroad because it authorized police to search for and seize any electronic device or digital media, even if the items had no connection to child pornography?
6. Was the warrant in this case overbroad because it granted police unfettered discretion to determine which items “pertain[ed] to” or “relate[d] to” child pornography, even if the material contained no images of children?

STATEMENT OF THE CASE

Microsoft reported to authorities that it “became aware that a user uploaded a media file believed to contain... suspected” child pornography. CP 23. Detective Eric Knudson traced the upload to a house in Walla Walla. CP 23-28. The house was occupied by a married couple (the Jensens), their son, and a housemate named Jay Friedrich. CP 24-25, 97. Knudson identified Mr. Friedrich as the likely suspect. CP 24-25.

Nearly a month after Microsoft became aware of the suspicious upload, Knudson obtained a warrant to search the Jensen residence for books, magazines, and other nondigital media. CP 35-36. The warrant authorized seizure of materials if they “pertain[ed] to” or “relate[d] to” child pornography, even if they contained no images of children. CP 35-36.

The warrant also authorized a search for electronic devices and digital media. CP 36-37. The warrant was intended to cover electronic devices and storage media owned or used by the Jensen family, if the police “determined that it is possible that the things described in this warrant could be found” on any of those devices. CP 29. The authorization to

search for digital evidence did not limit the search to child pornography. CP 36-37. Instead, it was intended to allow police to find “data that is capable of being read or interpreted by a computer,” even if the items and the data did not relate to child pornography. CP 36-37.

Although Knudson relayed the date that Microsoft “became aware” of the suspect upload, he did not say when the upload occurred. CP 23-24. He made numerous general assertions about the common habits of “pornographers,” “suspects,” “individuals that trade in this type of illegal activity,” and “child pornography collectors.”² CP 12-16.

Police executed the warrant, and Mr. Friedrich was charged with dealing in child pornography and possession of child pornography. CP 1-4. He moved to suppress the evidence, arguing that the warrant was overbroad under the Fourth Amendment and Wash. Const. art. I, §7. CP 5-10.

The trial court denied the motion to suppress. CP 74-75, 85-88. Mr. Friedrich stipulated to facts sufficient for conviction and was found guilty of one count of dealing in child pornography and four counts of possession. CP 76-84. He appealed, and the Court of Appeals affirmed his convictions in a published opinion.

² For example, Knudson claimed that collectors “sometimes possess and maintain their ‘hard copies’ of child pornographic material... in the privacy and security of their home or some other secure location, such as a private office.” CP 14. He alleged that such collectors “typically retain [child pornography] for many years,” and “prefer not to be without their child pornography for any prolonged time period.” CP 14-15.

ARGUMENT WHY REVIEW SHOULD BE ACCEPTED

I. THE SUPREME COURT SHOULD ACCEPT REVIEW TO RESOLVE AN INCONSISTENCY IN THE STANDARD FOR REVIEWING A MAGISTRATE'S DECISION TO ISSUE A SEARCH WARRANT.

The Supreme Court has repeatedly affirmed that a probable cause determination “is a legal question that is reviewed de novo.” *State v. Ollivier*, 178 Wn.2d 813, 848, 312 P.3d 1 (2013).³ However, the court has also said that “[t]he issuing magistrate’s determination of probable cause is reviewed for abuse of discretion and is given great deference by the reviewing court.” *State v. Maddox*, 152 Wn.2d 499, 509, 98 P.3d 1199 (2004).⁴

As Judge Fearing pointed out in his concurrence, “de novo review may conflict with granting the magistrate deference, let alone great deference.” *See* Opinion (Fearing, J., concurring) p. 2. The Supreme Court should accept review to resolve this inconsistency.

Review of a search warrant “is limited to the four corners of the affidavit supporting probable cause.” *Neth*, 165 Wn.2d at 182. Any judicial officer who examines a search warrant affidavit is presented with the same set of facts. Both the issuing magistrate and the reviewing court determine if the affidavit “sets forth facts and circumstances sufficient to establish a reasonable inference that the defendant is probably involved in criminal activity and that evidence of the crime may be found at a certain location.”

Jackson, 150 Wn.2d at 264.

³ *See also State v. Garcia-Salgado*, 170 Wn.2d 176, 183, 240 P.3d 153 (2010); *State v. Chamberlin*, 161 Wn.2d 30, 40, 162 P.3d 389 (2007); *State v. Neth*, 165 Wn.2d 177, 182, 196 P.3d 658 (2008).

⁴ *See also State v. Chenoweth*, 160 Wn.2d 454, 477, 158 P.3d 595 (2007); *State v. Lyons*, 174 Wn.2d 354, 362, 275 P.3d 314 (2012); *State v. Jackson*, 150 Wn.2d 251, 265, 76 P.3d 217, 225 (2003).

A probable cause determination is thus a pure question of law, subject to *de novo* review. *See, e.g., Town of Woodway v. Snohomish Cty.*, 180 Wn.2d 165, 172, 322 P.3d 1219 (2014). The Supreme Court’s admonition that “great deference” should be given to the magistrate’s determination is inconsistent with the legal nature of a probable cause determination.

Instead, any necessary “deference” is built into the *de novo* standard. This is because the affidavit must be reviewed “in a common sense manner, rather than hypertechnically.” *Jackson*, 150 Wn.2d at 265. Doubts are resolved in favor of the warrant. *Id.*, at 265.

The Supreme Court should clarify that probable cause determinations are reviewed *de novo*. This case presents a significant constitutional issue that is of substantial public interest. RAP 13.4(b)(3) and (4).

II. THE SUPREME COURT SHOULD ACCEPT REVIEW TO DETERMINE HOW COURTS SHOULD ASSESS STALENESS IN CASES INVOLVING SEARCH WARRANTS FOR DIGITAL IMAGES.

Although Detective Knudson based his warrant application on a suspicious upload, he could not say when the upload occurred. CP 23. Instead, without explanation, he gave the date Microsoft “became aware” of the upload. CP 23. Knudson’s request for authorization to search the Jensen residence came nearly a month after Microsoft “became aware” of the upload. CP 23-34. No evidence suggested that the upload had been accomplished through use of a device that remained at the house. CP 23-34.

Knudson’s affidavit did not provide probable cause, because the issuing magistrate had no way of knowing when the criminal activity occurred or if evidence remained at the Jensen residence. The allegations

were stale, and the items and images seized from the residence should have been suppressed.

A. Authorization to search a private residence may not rest on stale information.

Search warrants must be based on probable cause. U.S. Const. Amend. IV; Wash. Const. art I, §7;⁵ *Lyons*, 174 Wn.2d at 359. To establish probable cause, the warrant application “must set forth sufficient facts to convince a reasonable person of the probability the defendant is engaged in criminal activity and that evidence of criminal activity can be found at the place to be searched.” *Id.*

Stale information cannot establish probable cause. *Lyons*, 174 Wn.2d at 359-363. Courts consider the time elapsed since the known criminal activity and “the nature and scope of the suspected activity.” *Lyons*, 174 Wn.2d at 361. An issuing magistrate “cannot determine whether observations recited in the affidavit are stale unless the magistrate knows the date of those observations.” *Lyons*, 174 Wn.2d at 361. Ordinarily, two moments are critical: (1) when the officer received the information, and (2) when the informant observed the criminal activity. *Id.*

In *Lyons*, the warrant application omitted the second piece of information. *Id.*, at 363. The affidavit alleged that “[w]thin the last 48 hours a reliable and confidential source of information (CS) contacted [narcotics]

⁵ The state constitutional provision provides stronger protection than does the Fourth Amendment. *State v. Meneese*, 174 Wn.2d 937, 946, 282 P.3d 83 (2012). Accordingly, the six-part *Gunwall* analysis used to interpret state constitutional provisions is not necessary for issues relating to art. I, §7. *State v. White*, 135 Wn.2d 761, 769, 958 P.2d 962 (1998); *State v. Gunwall*, 106 Wn.2d 54, 720 P.2d 808 (1986).

Detectives and stated he/she observed narcotics, specifically marijuana, being grown indoors at the listed address.” *Id.*, at 363.

The Supreme Court concluded “this language ‘does not clearly state the time between the informant's observations and the filing of the affidavit.’” *Id.* (quoting lower court decision). The court determined that the warrant was not based on probable cause:

Because the affidavit for search warrant in this case did not relate when the confidential informant observed marijuana growing on Lyons' property, the affidavit did not provide sufficient support for the magistrate's finding of timely probable cause.

Id., at 368.

This case presents a problem related to that discussed in *Lyons*. Police knew when Microsoft “became aware” of the illegal upload; however, Knudson could not say when the upload occurred.

B. The warrant to search the Jensen residence rested on stale information.

As in *Lyons*, the affidavit here did not “provide sufficient support for the magistrate’s finding of *timely* probable cause.” *Id.* (emphasis added). But this deficiency is not identical to the problem in *Lyons*.

Here, the informant (Microsoft) “became aware” of criminal activity that had already occurred. CP 23. They “became aware” of the suspicious upload on March 30th, but nothing in the warrant affidavit indicates when the upload occurred. CP 23.

In *Lyons*, the informant directly observed a marijuana grow operation. *Id.*, at 363. *Lyons* would more directly resemble this case if the informant had observed a picture of a marijuana operation, without knowing

when the picture was taken. Such an informant could tell police the date she or he “became aware” of the illegal activity, but this language would not convey to the issuing magistrate when the activity took place.

Nor does the warrant application explain what it means for an entity like Microsoft to “become aware” of internet activity. The company may have “become aware” of the suspicious upload when a human technician reviewed information flagged by monitoring software days or weeks earlier. Federal law requires only that a company such as Microsoft report suspected child pornography “as soon as reasonably possible.” CP 18 (citing 18 U.S.C. §2258A(a)(1)).

As in *Lyons*, the affidavit lacks critical temporal information. Without knowing when the upload occurred, the issuing magistrate could not know if Knudson’s information was current or stale. This is especially problematic here because nearly a month passed between the report from Microsoft and the date Knudson applied for the warrant. CP 23, 30.

In addition, “the nature and scope of the suspected activity” weighs against a finding of probable cause. *Lyons*, 174 Wn.2d at 361. Microsoft flagged a single image upload that it “became aware” of a month prior to the warrant application. CP 23. Nothing in the affidavit suggests a high volume of illegal activity over a prolonged period. Given the “nature and scope” of the activity, the affidavit does not “provide sufficient support for the magistrate’s finding of *timely* probable cause.” *Id.* (emphasis added).

Phones, laptops, hard drives, and other such devices are highly portable. It is therefore irrelevant that information can persist on electronic

media, as Knudson outlines at length. CP 26-27. Electronic devices can easily be moved from one place to another. For example, a person may upload images using a borrowed phone or laptop; this does not mean that the borrowed device will be found at the person's house a month later.

The Court of Appeals did not address *Lyons*. It presumed that "Microsoft's detection and reporting would be prompt," without any evidence outlining the company's protocols for reviewing suspicious images. OP 10. Nothing shows that Microsoft allows software to automatically handle its reporting requirements without human intervention, or that it interprets the phrase "as soon as reasonably possible"⁶ in a manner that precludes the issuance of warrants based on stale information. The Court of Appeals also presumed that evidence remained at the Jensen home a month after Microsoft made its report, without any discussion of the inherent mobility of electronic devices and media.⁷ CP 12-16; OP 10-13.

The Supreme Court should accept review and reverse the Court of Appeals. The warrant affidavit did not permit the issuing magistrate to determine if the allegations of criminal activity were stale. *Id.* The appellate court's published decision conflicts with *Lyons*. In addition, this case presents a significant question of constitutional law that is of substantial public interest. RAP 13.4(b)(1), (3), and (4).

⁶ See 18 U.S.C. §2258A(a)(1).

⁷ In addition, the Court of Appeals approved Knudson's descriptions of the common habits of "child pornography collectors." CP 12-16; OP 10-13. This is discussed further.

III. THE SUPREME COURT SHOULD ACCEPT REVIEW AND REVERSE BECAUSE THE WARRANT APPLICATION RESTED PRIMARILY ON BROAD GENERALIZATIONS ABOUT THE COMMON HABITS OF “CHILD PORNOGRAPHY COLLECTORS.”

In his warrant application, Knudson devoted several pages to the general habits of “child pornography collectors” and others involved in “computer-related crimes.” CP 12-16. Based on this information, the court granted authority to search for many items unrelated to the single digital image flagged by Microsoft. CP 35-36. In addition, the generalities and blanket inferences were used to suggest that issues of staleness could safely be ignored. According to Knudson, child pornography allegations will never become stale, because collectors typically retain material “for many years” and “prefer not to be without their child pornography for any prolonged time period.”⁸ CP 15.

Standing alone, generalizations regarding common habits of criminals do not provide the individualized suspicion required to justify the issuance of a search warrant. *State v. Thein*, 138 Wn.2d 133, 147-149, 977 P.2d 582 (1999). This is consistent with the requirement that the affiant “must state the underlying facts and circumstances on which [the warrant application] is based in order to facilitate a detached and independent evaluation of the evidence by the issuing magistrate.” *Id.*, at 140.

Under the Fourth Amendment, generalizations based on the affiant’s experience may contribute to probable cause if paired with sufficient

⁸ Knudson’s generalizations do not necessarily apply to a person who *uploads* a suspect image, as opposed to a “collector” who downloads such images from the internet. There is no allegation here that an image was downloaded. CP 23. A person who uploads child pornography may not be a “child pornography collector.” CP 14.

facts.⁹ *Maddox*, 152 Wn.2d at 511. However, the Supreme Court has never determined if such a pairing survives analysis under Wash. Const. art. I, §7. The *Thein* court did not mention either the Fourth Amendment or Wash. Const. art. I, §7. Cases applying *Thein* have not distinguished between the state and federal constitutional provisions. *See, e.g., State v. Keodara*, 191 Wn. App. 305, 315-316, 364 P.3d 777 (2015), *review denied*, 185 Wn.2d 1028, 377 P.3d 718 (2016) (applying both constitutions).

Here, the Court of Appeals acknowledged that Knudson’s generalizations “warrant critical examination,” but accepted them because they “fall within the ambit of reasonableness.” OP 12. But “reasonableness” is a Fourth Amendment concept.

Unlike the Fourth Amendment, the state constitutional protection of an individual’s private affairs “is not grounded in notions of reasonableness.” *State v. Snapp*, 174 Wn.2d 177, 194, 275 P.3d 289 (2012). The “protections guaranteed by article I, section 7 of the state constitution are qualitatively different from those provided by the Fourth Amendment.” *State v. McKinney*, 148 Wn.2d 20, 26, 60 P.3d 46 (2002). Instead of “a downward ratcheting mechanism of diminishing expectations of privacy,” the state constitution “holds the line.” *State v. Ladson*, 138 Wn.2d 343, 349, 979 P.2d 833 (1999).

Here, the Court of Appeals relied on federal cases applying the Fourth Amendment to analyze Knudson’s generalizations. OP 12 (citing

⁹ The *Maddox* court explicitly limited its analysis to the federal constitution. *Maddox*, 152 Wn.2d at 505 n. 1.

United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005), *United States v. Burkhardt*, 602 F.3d 1202 (10th Cir. 2010), and cases cited therein). The court also noted that it had previously “found that ‘boilerplate’ inferences in a warrant affidavit provided probable cause that evidence of child pornography could be found at a suspect’s residence months after detecting his use.” OP 13 (citing *State v. Garbaccio*, 151 Wn. App. 716, 214 P.3d 168 (2009)).

But the *Garbaccio* court made no reference to the state constitution. Instead, it relied on federal authority to approve the use of boilerplate generalizations. *Garbaccio*, 151 Wn. App. at 729 (citing *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir.1997)).

The Supreme Court should accept review and hold that broad generalizations regarding the common habits of criminals may not be considered when evaluating probable cause under Wash. Const. art. I, §7. This case presents significant constitutional issues that are of substantial public interest. RAP 13.4(b)(3) and (4).

IV. THE SUPREME COURT SHOULD ACCEPT REVIEW AND REVERSE BECAUSE THE WARRANT WAS OVERBROAD.

Based on evidence of a single *digital* upload, Knudson obtained a warrant authorizing police to search for and seize (among other things) books, magazines, letters, negatives, film, and video cassettes. CP 35-36. Police were permitted to seize many items that merely “pertain[ed] to” or “relate[d] to” child pornography, even if the material did not contain any visual depictions of children. CP 35-36.

The warrant also authorized seizure of electronic devices and media that could contain “data that is capable of being read or interpreted by a computer,” even if the items and the data did not relate to child pornography. CP 36-37. The warrant was also intended to allow police to search for and seize “computers and other electronic devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime.” CP 29. Because the affidavit did not provide probable cause for these materials, the warrant was overbroad.

A. A warrant to search a private residence must be based on probable cause and must describe with scrupulous exactitude any items presumptively protected by the First Amendment.

General warrants are prohibited by the Fourth Amendment.

Steagald v. United States, 451 U.S. 204, 220, 101 S. Ct. 1642, 68 L. Ed. 2d 38 (1981). The warrant here amounted to a general warrant authorizing police to rummage through private papers and electronic data.

A search warrant is overbroad if it fails to describe the items to be seized with particularity. *State v. Perrone*, 119 Wn.2d 538, 545, 834 P.2d 611, 614 (1992). A warrant is also overbroad if it authorizes police to search for items in the absence of probable cause; in such cases, “no degree of particularity” will suffice. *Id.*, at 558; *see also State v. Higgs*, 177 Wn. App. 414, 426, 311 P.3d 1266, 1273 (2013), *as amended* (Nov. 5, 2013). A warrant is overbroad even if probable cause supports some portions of the warrant. *Higgs*, 177 Wn. App. at 426.

The probable cause and particularity requirements are “closely in-

tertwined.” *Perrone*, 119 Wn.2d at 545. The particularity requirement prevents “general searches,” the improper seizure of objects mistakenly believed to fall within the issuing magistrate’s authorization, and “the issuance of warrants on loose, vague, or doubtful bases of fact.” *Id.*, at 545.

A warrant authorizing seizure of materials protected by the First Amendment requires close scrutiny. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978); *Stanford v. Texas*, 379 U.S. 476, 485, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965); *Perrone* 119 Wn.2d at 547. In such cases, the particularity requirement must be “accorded the most scrupulous exactitude.” *Stanford*, 379 U.S. at 485.

Warrants targeting child pornography fall within this constitutional mandate. *Perrone*, 119 Wn.2d at 550. Even if they are ultimately determined to be illegal, the objects of such a search are materials presumptively protected by the First Amendment, and the heightened standards apply. *Id.*, at 547, 550.

In *Perrone*, the court found a search warrant “overly broad in its entirety.” *Perrone*, 119 Wn.2d at 542. The warrant authorized a search for items for which the police lacked probable cause.¹⁰ *Perrone*, 119 Wn.2d at 551-52. The *Perrone* warrant’s language also left the executing officer too much discretion, because it allowed “seizure of anything which the officer thinks constitutes ‘child pornography.’” *Id.* This, the court said, was not

¹⁰ These included “adult pornography, pornographic drawings, and sexual paraphernalia,” as well as depictions of children in sexually suggestive poses. *Perrone*, 119 Wn.2d at 551-52.

the “scrupulous exactitude” required for seizure of materials presumptively protected by the First Amendment. *Id.*

Here, as in *Perrone*, Knudson sought materials presumptively protected by the First Amendment. Because of this, the particularity requirement must be “accorded the most scrupulous exactitude.” *Perrone*, 119 Wn.2d at 547-548 (quoting *Stanford*, 379 U.S. at 485).

B. The warrant application did not supply probable cause for numerous items listed in the warrant, including material protected by the First Amendment.

Detective Knudson received information regarding a single digital image. CP 23. Based on this, he sought and received authorization to search for books, magazines, documents, negatives, film, video cassettes, and other non-digital material. CP 35-36. Police were authorized to seize many items that merely “pertain[ed] to” or “relate[d] to” child pornography, including material that did not contain any visual depictions of children. CP 35-36.

The warrant was unconstitutionally overbroad: nothing suggested that police would find non-digital media containing child pornography. *Perrone*, 119 Wn.2d at 547-548. The affidavit did not supply probable cause to search for and seize books, magazines, film, video cassettes and so forth, because the information provided by Microsoft related to a single digital image. CP 23.

The Court of Appeals has previously found a warrant overbroad under similar circumstances. *State v. Griffith*, 129 Wn.App. 482, 488-489,

120 P.3d 610 (2005). The Court of Appeals' published decision here conflicts with *Griffith*.

In *Griffith*, police learned that the defendant had taken photographs of an underage guest at his birthday party and had transferred them from a digital camera to a computer. *Griffith*, 129 Wn. App. at 486. Instead of seeking authorization to search for and seize the defendant's digital camera and computers, police obtained a warrant to search for "all cameras—digital, 35 millimeter, and Polaroid—unprocessed film, all computer processing units and all electronic storage media, documents pertaining to internet accounts, all material depicting a minor engaged in sexually explicit conduct, printed material showing the exposed genitals or rectal area of a minor, videotapes, digital images, and any documents relating to the distribution or receipt of child pornography." *Id.* at 488-489.

The *Griffith* court found the warrant overbroad. *Id.* As there, police here obtained permission to seize numerous non-digital items unconnected to the single digital upload that prompted their investigation. CP 23, 35-36. The warrant authorized investigators to rummage through the household's books, magazines, films, videos, and other analog media. Even so, the appellate court concluded that the warrant "was not overbroad as to media whose content could be assessed during the search." OP 18.

The Court of Appeals' Published Opinion conflicts with *Perrone* and *Griffith*. In addition, this case presents significant constitutional issues that are of substantial public interest. The Supreme Court should accept review. RAP 13.4(b)(1), (2), (3), and (4).

C. The warrant failed to particularly describe most of the material subject to seizure, including items protected by the First Amendment.

In examining a warrant, “the degree of specificity required varies according to the circumstances and the type of items involved.” *Perrone*, 119 Wn.2d at 546. In addition, “[g]reater particularity is required where First Amendment considerations are concerned.” *Id.*, at 553. In this case, the warrant included two categories of items to be seized: “Records, Documents, and Visual Depictions” and “Digital Evidence.” CP 35-37. The language describing both categories fails the particularity requirement.

Many subcategories of “Records, Documents, and Visual Depictions” allowed police to search for and seize those items that “pertain to” or “relate to” “visual depictions of minors engaged in sexually explicit conduct.”¹¹ CP 35-36. These descriptions were insufficiently particular under both the Fourth Amendment and Wash. Const. art. I, §7.

The warrant allowed officers unfettered discretion to determine what it means to “pertain to” or “relate to” illegal visual depictions of children. *See Perrone*, 119 Wn.2d at 553. It authorized police to seize many items that did not contain any images if the executing officers believed the material pertained to or related to child pornography. CP 35-36.

To paraphrase *Perrone*, “a description authorizing seizure of anything which the officer thinks [pertains to or relates to illegal images]

¹¹ As outlined above, the police lacked probable cause to search for these items; they had no information suggesting that child pornography would be found in paper form or any of the other non-digital items described.

leaves the executing officer with too much discretion, and is not ‘scrupulous exactitude.’” *Id.*, at 553. As in *Perrone*, the warrant here was unconstitutionally overbroad, because it authorized seizure of items protected by the First Amendment without describing them with particularity. *Id.*

The “Digital Evidence” subcategories did not even contain the inadequate limitation applied to the non-digital categories. CP 36-37. Instead, the warrant authorized police to “seize, image, copy, and/or search” all electronic devices and digital media,¹² even if it did not relate to visual depictions of children engaged in sexually explicit conduct.¹³ CP 36-37.

The goal of this authorization was to enable police “to search for *data* that is capable of being read or interpreted by a computer.” CP 36 (emphasis added). The warrant placed no limitation on the kind of data to be sought. The warrant’s description of “Digital Evidence” is insufficiently particular; it cannot withstand constitutional scrutiny. *Id.* The warrant amounts to a general warrant “for data,” even if it has no connection to depictions of children engaged in sexually explicit conduct.¹⁴

¹² In addition, the “Digital Evidence” category authorized seizure of items incapable of storing data (such as keyboards and cables) and printed material such as reference manuals. CP 36-37.

¹³ Item “h” authorized seizure of information showing the identity of the user during the time the device was used in connection with “child pornography.” CP 37. The *Perrone* court found the phrase “child pornography” insufficient: “a description authorizing seizure of anything which the officer thinks constitutes ‘child pornography’ leaves the executing officer with too much discretion, and is not ‘scrupulous exactitude.’” *Perrone*, 119 Wn.2d at 553.

¹⁴ This is in addition to the authorization to seize keyboards, reference manuals, and other physical items incapable of storing images or other data. CP 36-37.

The Court of Appeals excused this deficiency by adopting what it described as “the most reasonable approach” for seizing digital evidence.¹⁵ OP 19. But “reasonableness” is a Fourth Amendment concept, inconsistent with the requirements of Wash. Const. art. I, §7. *Snapp*, 174 Wn.2d at 194; *McKinney*, 148 Wn.2d at 26.

The court failed to address the absence of any limitation on the seizure of digital media. Police were not required to seize only those items suspected to contain illegal images; instead, they were authorized to seize anything that could contain “data” (as well as keyboards, cables, and other items that could not contain data.) CP 36-37.

Furthermore, even if the descriptions had included some limitation, Washington courts applying the state constitution should not accept “the reality that over-seizing is an inherent part of the electronic search process.” *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010), *abrogated in part on other grounds by Hamer v. Neighborhood Hous. Servs. of Chicago*, --- U.S. ---, 138 S. Ct. 13, 199 L. Ed. 2d 249 (2017); OP 19.

The warrant violated the particularity requirement. *Perrone*, 119 Wn.2d at 546-556. It authorized police to determine which non-digital items “pertain[ed] to” or “relate[d] to” child pornography. CP 35-36. It also allowed police to seize electronic devices and media to search “for

¹⁵ [T]he most reasonable approach would appear to be to authorize seizure of all reasonably suspect devices, but with a particularized protocol for searching the devices following the seizure.” OP 19. The court also upheld Mr. Friedrich’s conviction through a misapplication of the severability doctrine, as outlined below.

data that is capable of being read or interpreted by a computer,” without any limitation. CP 36. Evidence seized pursuant to the warrant should have been suppressed. *Id.*

The Court of Appeals decision conflicts with *Perrone*. This case presents significant constitutional issues of substantial public interest. The Supreme Court should accept review. RAP 13.4(b)(1), (3) and (4).

D. The Court of Appeals misapplied the severability doctrine.

The severability doctrine permits a reviewing court to distinguish valid portions of the warrant from invalid portions. *Perrone*, 119 Wn.2d at 556. Contrary to the Court of Appeals’ conclusion, the doctrine requires more than simply examining the evidence admitted at trial to determine if valid portions of the warrant authorized its seizure. OP 19-20.

The severability doctrine only applies where “a meaningful separation to be made of the language in the warrant.” *Id.*, at 560. Invalid portions of a warrant may be severed when there is “some logical and reasonable basis for the division of the warrant into parts which may be examined for severability.” *Id.* In addition:

[a]t a minimum, where materials presumptively protected by the First Amendment are concerned, the severance doctrine should only be applied where discrete parts of the warrant may be severed, and should not be applied where extensive ‘editing’ throughout the clauses of the warrant is required to obtain potentially valid parts.

Id. The Court of Appeals ignored this restriction. OP 19-20. The *Griffith* court made a similar error. *Griffith*, 129 Wn. App. at 489 (“Under the severability doctrine, only the invalid portions of the warrant must be suppressed.”) The warrant here cannot be divided into “discrete parts” that

can be severed from the remainder.¹⁶ *Perrone*, 119 Wn.2d at 560. The description of digital evidence allowed police to seize anything that could contain “data” (as well as items such as keyboards and cable that could not). CP 36-37.

The description of non-digital materials consists entirely of items for which police lacked probable cause. Furthermore, many of the subcategories impermissibly allowed seizure of items that merely “pertain[ed] to” or “relate[d] to” child pornography. CP 35-36. This language is insufficiently particular and allowed the executing officers too much discretion, as outlined above.

There is no “logical and reasonable basis for the division of the warrant into parts which may be examined for severability.” *Id.* Instead, “the substantial editing required here... is flatly inconsistent” with the requirement that items presumptively protected by the First Amendment be described with scrupulous exactitude. *Id.*, at 560–561.

The Court of Appeals’ application of the severability doctrine conflicts with *Perrone*. Furthermore, this case presents significant constitutional issues that are of substantial public interest. The Supreme Court should accept review. RAP 13.4(b)(1), (3) and (4).

¹⁶ The sole exception relates to the nine IP addresses outlined in Section 3. CP 37. However, the authorization to search for evidence relating to those nine IP addresses contributes to the overall overbreadth of the warrant.

CONCLUSION

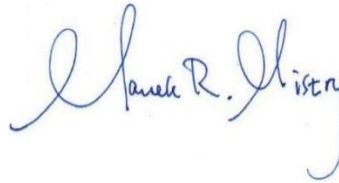
For the foregoing reasons, the Supreme Court should accept review, reverse the Court of Appeals, and remand with instructions to suppress the evidence.

Respectfully submitted September 24, 2018.

BACKLUND AND MISTRY



Jodi R. Backlund, No. 22917
Attorney for the Appellant



Manek R. Mistry, No. 22922
Attorney for the Appellant

CERTIFICATE OF SERVICE

I certify that I mailed a copy of the Petition for Review, postage pre-paid, to:

Jay Friedrich, DOC #824566
Stafford Creek Corrections Center
191 Constantine Way
Aberdeen, WA 98520

and I sent an electronic copy to

Walla Walla County Prosecuting Attorney
jnagle@co.walla-walla.wa.us
tchen@co.franklin.wa.us

through the Court's online filing system, with the permission of the recipient(s).

In addition, I electronically filed the original with the Court of Appeals.

I CERTIFY UNDER PENALTY OF PERJURY UNDER THE LAWS OF THE STATE OF WASHINGTON THAT THE FOREGOING IS TRUE AND CORRECT.

Signed at Olympia, Washington on September 24, 2018.



Jodi R. Backlund, WSBA No. 22917
Attorney for the Appellant

APPENDIX:

Court of Appeals Published Opinion filed on August 23, 2018.

FILED
AUGUST 23, 2018
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. 35099-1-III
Respondent,)	
)	
v.)	
)	
JAY KARL FRIEDRICH,)	PUBLISHED OPINION
)	
Appellant.)	

SIDDOWAY, J. — Anyone engaged in “providing an electronic communication service or a remote computing service” to the public in interstate commerce is required to report any known child pornography violation to an electronic tip line, where it is made available to law enforcement. *See* 18 U.S.C. § 2258A. Jay Friedrich was convicted of five counts of dealing with or possessing depictions of a minor engaged in sexually explicit conduct after Microsoft filed such a report, which was investigated by the Walla Walla County sheriff.

Mr. Friedrich appeals denial of his motion to suppress the critical evidence against him. He argues that the information reported by Microsoft and the warrant affidavit’s generalizations about collectors of child pornography did not provide probable cause for

a search of his residence and that the affidavit failed to satisfy the particularity required by the Fourth Amendment to the United States Constitution.

The totality of information provided by the affidavit, including commonsense inferences about where and how long child pornography is likely to be retained, provided probable cause to issue the warrant. For that reason, and because any issue of overbreadth is avoided by the severability doctrine, we affirm.

FACTS AND PROCEDURAL BACKGROUND

On March 30, 2016, Microsoft reported to the National Center for Missing and Exploited Children (NCMEC)¹ that it became aware that a user of Skype,² user name “jkf6418,” uploaded a media file believed to contain a depiction of a minor engaging in sexually explicit conduct. Clerk’s Papers (CP) at 23. Microsoft’s report indicated that a search of Skype for the username “jkf6418” yielded three results, all belonging to a “Jay Friedrich.” *Id.* The one result identifying “Jay Friedrich[’s]” city of residence identified it as Walla Walla, Washington. The NCMEC report indicated that a search of the

¹ NCMEC is a national resource center and clearinghouse that maintains an electronic tip line, the “CyberTipline,” through which federally-required reports are transmitted to the appropriate international, federal, and local law enforcement agencies for investigation. 42 U.S.C. §§ 5771, 5773(b). Providers who fail to comply with the reporting obligation face substantial penalties. *See* 18 U.S.C. § 2258A; *United States v. Ackerman*, 831 F.3d 1292, 1296-97 (10th Cir. 2016).

² Skype is a telecommunications application for video chats, voice calls, or instant messaging. *See About Skype*, SKYPE, <https://www.skype.com/en/about> [<https://perma.cc/LL58-566K>].

username “jkf6418” on Spokeo, a people search website that aggregates data from other services, also yielded three results. One, a dating profile on an online dating site, described “jkf6418” as a 51-year-old bisexual single male from Walla Walla and as 6’1” and of average build.

After it was determined that the Internet Protocol (IP) address most likely came from Walla Walla, the information was passed along to the Walla Walla County Sheriff’s Department and investigation of the report was referred to Detective Eric Knudson on April 12. Detective Knudson viewed the media file, a picture of what appeared to be an approximately 9- to 11-year-old girl engaged in “sexually explicit . . . conduct” as defined by RCW 9.68A.011(4). CP at 24.

On April 13, Detective Knudson obtained a search warrant to locate the subscriber information for the IP address, which was registered to Charter Communications. Charter Communications responded to the warrant on April 21, identifying the service subscriber as Jay Jensen. Detective Knudson learned from a search of police records that in 2012 Jay Jensen reported finding child pornography on his roommate’s computer. The report listed Mr. Jensen’s roommate as Jay Friedrich. Mr. Friedrich was not charged as a result of that report, as the investigation produced insufficient evidence for prosecution. Detective Knudson nonetheless reviewed the pictures obtained in the investigation and determined that they were of teenage and preteen girls. Detective Knudson’s research also revealed that Mr. Friedrich is a registered sex offender.

Detective Knudson learned from police records that Mr. Friedrich lived in Walla Walla and was described as 52 years of age, 6'1" in height, and as weighing 155 pounds. His birthdate was recorded as 04/18/1964, which, along with his initials, jkf, correlated to the "jkf6418" account (04/18/1964).

A month after NCMEC received the report from Microsoft, on April 27, Detective Knudson applied for a warrant to search Mr. Friedrich's residence. In his 24-page supporting affidavit, Detective Knudson provided his background and training, the foregoing information, and information on the typical operational practices of electronic and internet service providers (collectively "ISPs"). He testified that pursuant to terms of their user agreements, ISPs "typically monitor their services utilized by subscribers[t]o prevent their communication networks from serving as conduits for illicit activity" and "routinely and systematically attempt to identify suspected child pornography that may be sent through [the ISP's] facilities." CP at 17. He testified that when an image or video file is believed by an ISP to be child pornography as defined by 18 U.S.C. § 2256, a "hash value" of the file can be generated by operation of a mathematical algorithm that is unique to the file—"in essence, the unique fingerprint of that file." CP at 17. A database of hash values for files suspected to be child pornography enables ISPs to automatically detect when files that have been identified as illicit pass through their system. He testified that reports to NCMEC by ISPs are often made solely on the basis of detection of a file's hash value.

In addition to describing these practices (although in more detail), Detective Knudson’s affidavit stated that under federal law, an ISP “has a duty to report to NCMEC any apparent child pornography it discovers ‘as soon as reasonably possible.’” CP at 18 (quoting 18 U.S.C. § 2258A(a)(1)).

The items that Detective Knudson sought to search for and seize were identified in two single-spaced pages of an attachment to his affidavit. They consisted of two categories: “Records, Documents, and Visual Depictions,” and “Digital Evidence.” CP at 32-33.

The requested search warrant was issued by District Court Judge Kristian Hedine on April 27. The last, freestanding provision of its digital evidence section authorized the seizure of records and things evidencing the use of nine IP addresses that were unrelated to Microsoft’s report to NCMEC. They were not identified or explained by Detective Knudson’s affidavit or its attachments.

In executing the search warrant the next day, law enforcement seized a Hewlett Packard laptop, a Toshiba laptop, a Micron tower computer, flash drives, compact disks, and floppy disks—all found in Mr. Friedrich’s bedroom. They seized a Samsung smartphone from Mr. Friedrich’s person. During an interview with officers, Mr. Friedrich admitted that the electronics seized were his and that they would contain images of underage girls. The Hewlett Packard computer and the Samsung smartphone proved to contain depictions of minors engaged in sexually explicit conduct, including

the image Microsoft reported. The Toshiba laptop and Micron tower computer also contained such depictions.

The State eventually charged Mr. Friedrich with one count of second degree dealing in depictions of a minor engaged in sexually explicit conduct, three counts of first degree possession of depictions of a minor engaged in sexually explicit conduct, and one count of second degree possession of depictions of a minor engaged in sexually explicit conduct, all in violation of RCW 9.68A.050 and .070. For simplicity's sake hereafter, and unless indicated otherwise, our references to "child pornography" are to depictions of minors whose possession or dealings with which violate provisions of chapter 9.68A RCW or federal law.

Mr. Friedrich moved the court to suppress all of the State's evidence, arguing that Detective Knudson's affidavit supporting his application did not meet the particularity requirement of the Fourth Amendment. The superior court, the Hon. John Lohrmann, denied the motion without a hearing. The parties then proceeded to a stipulated facts trial, with Mr. Friedrich preserving his right to appeal the trial court's suppression decision. Mr. Friedrich was convicted on all remaining counts. He appeals.

ANALYSIS

Mr. Friedrich's assignments of error present two challenges to the trial court's suppression decision. He contends first, that the warrant application failed to provide facts supporting a determination that what was at least month-old evidence of criminal

activity could still be found at his residence. His second contention is that the search warrant failed to satisfy the particularity requirement of the Fourth Amendment.

I. THE DISTRICT COURT COULD REASONABLY CONCLUDE THAT THE EVIDENCE OF CRIMINAL ACTIVITY WAS NOT STALE

Mr. Friedrich does not question that the warrant affidavit provided probable cause that he engaged in criminal activity at some time. But he cites two aspects of Detective Knudson's affidavit that he argues undermine probable cause that evidence of the criminal activity existed at Mr. Friedrich's residence at the time the detective applied for the search warrant. The first is the fact that the March 30, 2016 date of Microsoft's report to the CyberTipline was the date Microsoft "*became aware* that a user uploaded a media file," not the date of the upload itself. CP at 23 (emphasis added). The second is that four weeks had passed between Microsoft's report and the application for the warrant, and the detective's contention that the evidence would still be at the residence depended on unreliable generalizations about the habits of child pornography collectors.

The Fourth Amendment to the United States Constitution and article I, section 7 of the Washington Constitution require that the issuance of a search warrant be based on a determination of probable cause. Probable cause is established when an affidavit supporting a search warrant provides sufficient facts for a reasonable person to conclude there is a probability the defendant is involved in the criminal activity and that evidence

of the crime is at a certain location. *State v. Vickers*, 148 Wn.2d 91, 108, 59 P.3d 58 (2002).

Whether a warrant affidavit's information constitutes probable cause is a question of law that we review de novo. *State v. Neth*, 165 Wn.2d 177, 182, 196 P.3d 658 (2008). Nonetheless, in determining that question of law, “[g]reat deference is accorded the issuing magistrate’s determination of probable cause.” *State v. Cord*, 103 Wn.2d 361, 366, 693 P.2d 81 (1985). If the propriety of issuing the warrant is debatable, the deference due the magistrate’s decision will tip the balance in favor of upholding the warrant. *State v. Jackson*, 102 Wn.2d 432, 446, 688 P.2d 136 (1984). In light of the deference owed the magistrate’s decision, the question on review is whether the magistrate could draw the connection, not whether he should do so.

In reviewing a magistrate’s determination of probable cause, we—like the magistrate—should not view the affidavit “in a hypertechnical manner.” *State v. Riley*, 34 Wn. App. 529, 531, 663 P.2d 145 (1983). “[A] magistrate is entitled to draw reasonable inferences from the facts and circumstances set forth in the supporting affidavit,” with the result that “[r]easonableness is the key and common sense must be the ultimate yardstick.” *Id.* “Doubts concerning the existence of probable cause are generally resolved in favor of issuing the search warrant.” *Vickers*, 148 Wn.2d at 108-09.

Timeliness of Microsoft's detection and report

A passage of time between an observation of criminal activity and the presentation of a search warrant affidavit may be so prolonged that it is no longer probable that a search will reveal criminal activity or evidence; i.e., the information may be stale. *State v. Lyons*, 174 Wn.2d 354, 360-61, 275 P.3d 314 (2012). But “the information is not stale for purposes of probable cause if the facts and circumstances in the affidavit support a commonsense determination that there is continuing and contemporaneous possession of the property intended to be seized.” *State v. Maddox*, 152 Wn.2d 499, 506, 98 P.3d 1199 (2004).

Detective Knudson's affidavit stated that Microsoft's report indicated that it “became aware” of Mr. Friedrich's upload on March 30. CP at 23. It also informed the magistrate that ISPs such as Microsoft typically monitor their services to prevent their communication networks from serving as conduits for illicit activity, including to systematically attempt to identify suspected child pornography. He described the generation of hash values for pornographic files that enable ISPs to automatically detect the passage of some pornographic files through their system. Detective Knudson also cited federal law under which an ISP “has a duty to report to NCMEC any apparent child pornography it discovers ‘as soon as reasonably possible.’” CP at 18 (quoting 18 U.S.C. § 2258A(a)(1)). Mr. Friedrich concedes that “[p]resumably, Microsoft complied with this requirement.” Br. of Appellant at 15 n.11.

Industry practices exist, can often be determined by outsiders to the industry, and the practices described by Detective Knudson's affidavit are matters of which a detective with training in investigating child pornography cases could be expected to be aware. The district court judge was entitled to rely on the detective's knowledge of industry practice. That information and the federal reporting requirement support the magistrate's commonsense conclusion that Microsoft's detection and reporting would be prompt.

Likelihood that evidence of criminal activity would be located at Mr. Friedrich's residence

To establish the likelihood that evidence of criminal activity would still be located at Mr. Friedrich's residence, Detective Knudson's affidavit relied in part on the fact that digitized information will remain on a computer not only until deleted, but even thereafter, which Mr. Friedrich does not dispute.

Detective Knudson's affidavit also included generalizations about what collectors of child pornography generally do, which, according to the deputy, includes "prefer[ing] not to be without their child pornography for any prolonged time period," often maintaining photographs or videos "in computer files or external digital storage devices," and maintaining pornographic materials "in the privacy and security of their home or in some other secure location, such as a private office." CP at 14-15. Mr. Friedrich challenges these generalizations as support for a determination of probable cause, citing *State v. Thein*, 138 Wn.2d 133, 977 P.2d 582 (1999).

In *Thein*, our Supreme Court held that an officer's asserted understanding of the common habits of drug dealers was insufficient to establish probable cause to search the defendant's residence. The warrant affidavit in *Thein* presented specific facts providing probable cause that the defendant was a drug dealer, but only generalizations in support of the officer's belief that evidence of his criminal activity could be found at his residence. The court concluded that the generalized statements "in [Thein's] case were, standing alone, insufficient to establish probable cause to search [his] residence." *Id.* at 148. Although allowing that "common sense and experience inform the inferences reasonably to be drawn from the facts," the Court determined that the type of "broad generalizations" presented by the warrant affidavit for Thein's residence "do not alone establish probable cause." *Id.* at 148-49.

The Court added a cautionary note, "emphasiz[ing] that the existence of probable cause is to be evaluated on a case-by-case basis" and in each case, "'the facts stated, the inferences to be drawn, and the specificity required must fall within the ambit of reasonableness.'" *Id.* at 149 (quoting *State v. Helmka*, 86 Wn.2d 91, 93, 542 P.2d 115 (1975)). More recently, our Supreme Court observed in *Maddox* that "[i]n evaluating whether the facts underlying a search warrant are stale, the court looks at the totality of circumstances," including "the nature and scope of the suspected criminal activity." 152 Wn.2d at 506.

Detective Knudson's generalizations about what possessors of child pornography

“generally do” warrant critical examination for the reasons given in *Thein*. But unlike the generalizations about drug dealers in *Thein*, Detective Knudson’s generalizations about possessors of child pornography fall within the ambit of reasonableness, and similar generalizations have survived critical examination in a number of courts. In a relatively early case involving a warrant to search for digital evidence of child pornography at a user’s residence, the federal appellate court for the Tenth Circuit Court of Appeals endorsed a view that possessors of child pornography are likely to hoard materials and maintain them for significant periods of time, explaining that the view

“is supported by common sense and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence.”

United States v. Riccardi, 405 F.3d 852, 861 (10th Cir. 2005) (quoting *United States v. Lamb*, 945 F. Supp. 441, 460 (N.D.N.Y. 1996)).

The Tenth Circuit abided by that view five years later, despite an intervening increase in internet access to child pornography that made it easier to anonymously collect and possess it. In *United States v. Burkhart*, the court explained:

[C]hild pornography is still illegal to distribute and possess, and still carries severe social stigma, whether the possessor receives it by regular mail, email, or over the Internet. The illegality and social stigma may also complicate resale or disposal. Moreover, acquiring pornography is rarely free. Given the nature of the evidence to be seized, the Internet context may mitigate *against* staleness: information that a person received

electronic images of child pornography is less likely than information about drugs, for example, to go stale because the electronic images are not subject to spoilage or consumption.

602 F.3d 1202, 1207 (10th Cir. 2010) (citing *United States v. Frechette*, 583 F.3d 374, 378 (6th Cir. 2009)). *Burkhart* points out that at the time of its filing, it was one of five federal circuit courts that had endorsed the observation that possessors of child pornography are likely to hoard it. *Id.*³ This court also found that “boilerplate” inferences in a warrant affidavit provided probable cause that evidence of child pornography could be found at a suspect’s residence months after detecting his use. *State v. Garbaccio*, 151 Wn. App. 716, 729, 214 P.3d 168 (2009), relying on *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997).

Probable cause requires more than suspicion or conjecture, but it does not require certainty. *State v. Chenoweth*, 160 Wn.2d 454, 476, 158 P.3d 595 (2007). Because common sense and experience supports the generalizations presented by Detective Knudson, the district court could reasonably find a fair probability that possessors of child pornography are likely to retain the material for a considerable period of time in a secure location, such as the possessor’s home.

³ In addition to the Sixth Circuit decision in *Frechette*, *Burkhart* cited *United States v. McArthur*, 573 F.3d 608, 613-14 (8th Cir. 2009); *United States v. Falso*, 544 F.3d 110, 132 (2d Cir. 2008); and *United States v. Watzman*, 486 F.3d 1004, 1008 (7th Cir. 2007).

II. THE SEARCH WARRANT SATISFIED THE CONSTITUTIONAL PARTICULARITY REQUIREMENT IN MOST RESPECTS, AND THE ITEMS SEIZED FALL WITHIN ITS LEGITIMATE SCOPE

Mr. Friedrich’s remaining argument is that the search warrant was vague, overbroad, and sought materials presumptively protected by the First Amendment to the United States Constitution.

Among the requirements of the Fourth Amendment is that no warrant shall issue without “*particularly describing* the place to be searched, and the persons or things to be seized.” U.S. CONST. AMEND. IV (emphasis added); *State v. Riley*, 121 Wn.2d 22, 28 n.1, 846 P.2d 1365 (1993). “The purposes of the search warrant particularity requirement are the prevention of general searches, prevention of the seizure of objects on the mistaken assumption that they fall within the issuing magistrate’s authorization, and prevention of the issuance of warrants on loose, vague, or doubtful bases of fact.” *State v. Perrone*, 119 Wn.2d 538, 545, 834 P.2d 611 (1992) (citing, among other authority, *Marron v. United States*, 275 U.S. 192, 48 S. Ct. 74, 72 L. Ed. 231 (1927)).

The first two purposes are related. The first prevents the sort of general, exploratory rummaging in a person’s belongings of the sort “‘abhorred by the colonists.’” *Id.* (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971)). The second ensures that what is to be seized is determined by a neutral magistrate, eliminating the danger of unlimited discretion in the executing officer. *Id.* at 546. As to these related purposes, “a description is valid if it is as specific as the

circumstances and the nature of the activity under investigation permits.” *Perrone*, 119 Wn.2d at 547.

A greater degree of particularity is required when a search warrant authorizes a search for items protected by the First Amendment. *Id.* at 547. Describing the history of this heightened requirement in 1965, the U.S. Supreme Court stated that “[T]he most scrupulous exactitude” applies “when the ‘things [to be seized]’ are books, and the basis for their seizure is the ideas which they contain.” *Stanford v. Texas*, 379 U.S. 476, 485, 85 S. Ct. 506, 13 L. Ed. 2d 431 (cited by *Perrone*, 119 Wn.2d at 547-48).

The third purpose of the particularity requirement ties it to the requirement of probable cause. Imprecision in the description of the items to be seized that can be traced to “loose, vague, or doubtful bases of fact” increases the likelihood that probable cause has not been established. *Perrone*, 119 Wn.2d at 548. As to all three purposes, “[w]hether a search warrant contains a sufficiently particularized description is reviewed de novo.” *Id.* at 549.

The first infirmity alleged by Mr. Friedrich for his particularity challenge is the search warrant’s use of the unqualified term “child pornography” in one instance, in describing items to be seized. Use of the unqualified term proved fatal to the search warrant at issue in *Perrone*, in which the warrant affidavit repeatedly used the term to describe items to be seized, and our Supreme Court held that the term was “not sufficiently particular to satisfy the Fourth Amendment.” 119 Wn.2d at 553. The court

reasoned that authorizing law enforcement to seize anything it thinks constitutes “child pornography” allows for too much discretion and is not “scrupulous exactitude.” *Id.* (internal quotation marks omitted). The court suggested that a warrant affiant could avoid the particularity problem by using statutory definitions found in RCW 9.68A.011.⁴ *Id.* at 553-54. More recently, the Court reiterated that if a search warrant limiting items to be seized “used the *language* of RCW 9.68A.011 *to describe materials sought*, the warrant would likely be sufficiently particular,” but that merely identifying the crime under investigation as a violation of RCW 9.68A.070 did not satisfy the particularity requirement. *State v. Besola*, 184 Wn.2d 605, 614, 359 P.3d 799 (2015).

The search warrant in this case consistently qualified the “Records, Documents, and Visual Depictions” to be searched for and seized as ones containing, or pertaining or relating to, “visual depictions of minors engaged in sexually explicit conduct, as defined in RCW 9.68A.011 and Title 18, United States Code, Section 2256.” CP at 32. All items to be searched and seized were also qualified by introductory language that they be “records, documents, and items that constitute evidence, contraband, fruits, and/or instrumentalities of violations of RCW 9.68A.050, dealing in depictions of minor [sic] engaged in sexually explicit conduct.” CP at 35. The unqualified term “child

⁴ Chapter 9.68A RCW covers sexual exploitation of children, and section 9.68A.011 is its definitions provision.

pornography” appears only once, in authorizing seizure of materials “that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess or view child pornography.”

CP at 37. Given the introductory language and the consistent use of statutory definitions elsewhere, Mr. Friedrich’s attack is hypertechnical. The search warrant in this case does not present the infirmity presented by the search warrant in *Perrone*.

Additional and related infirmities alleged by Mr. Friedrich are the breadth of the media to be seized, which includes, e.g., books, magazines, photographs, motion picture films and videos; and the warrant’s extension to every digital device found in the residence that is “capable of storing and/or processing data in digital form,” as well as “related communications devices,” examples of which are provided. CP at 36. He argues that the breadth of both categories authorizes the seizure of items unrelated to the suspected crime, which was a single instance of uploading a digital image. Finally, he points to the fact that the search warrant authorized seizure of records and things evidencing the use of nine IP addresses having no apparent relation to Detective Knudson’s evidence.

The State responds that the particularity requirement tolerates ambiguity when the description is as complete as can be reasonably expected, and that the complaint about the breadth of devices whose seizure was authorized fails to consider that “[t]he only way police will know whether digital evidence contains child pornography is by seizing the

device and then submitting it to . . . expert examination. This cannot be ascertained at the time of seizure.” Br. of Resp’t at 19-20.

The State does not defend the provision of the search warrant dealing with the nine unexplained IP addresses, lending credence to Mr. Friedrich’s surmise that it was carryover language from an earlier search warrant. We set aside that provision for now, and address it in our concluding discussion of the severability doctrine.

As to the breadth of the types of media to be seized, “courts evaluating alleged particularity violations have distinguished between property that is inherently innocuous and property that is inherently illegal.” *State v. Chambers*, 88 Wn. App. 640, 644, 945 P.2d 1172 (1997) (internal quotation marks omitted). “A lesser degree of precision may satisfy the particularity requirement when a warrant authorizes the search for contraband or inherently illicit property.” *Id.* Child pornography is not protected by the First Amendment. *New York v. Ferber*, 458 U.S. 747, 102 S. Ct. 3348, 73 L. Ed. 2d 1113 (1982). The search warrant authorized a search for and seizure of only media containing statutorily-defined child pornography. It was not overbroad as to media whose content could be assessed during the search.

The breadth of digital devices to be seized presents a different issue because, as the State points out, whether they contained child pornography could not be assessed while executing the warrant at the residence. If a magistrate reasonably finds it probable that an individual has engaged in criminal dealings with child pornography, and digital

evidence of those dealings is likely to be found in devices located in his or her home, the most reasonable approach would appear to be to authorize seizure of all reasonably suspect devices, but with a particularized protocol for searching the devices following the seizure. *See, e.g., United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (per curiam) (en banc) (recognizing “the reality that over-seizing is an inherent part of the electronic search process”), *abrogated in part on other grounds by Hamer v. Neigh. Hous. Serv. Of Chi.*, ___ U.S. ___, 138 S. Ct. 13, 16-17, 199 L. Ed. 2d 249 (2017); *id.* at 1178-80 (Kozinski, C.J., concurring) (providing guidance on what magistrates should consider in issuing a warrant to examine an electronic storage medium to search for certain incriminating files).

The severability doctrine spares us the task of drawing lines about over-seizing electronic information in this case, because the evidence that was seized and used to convict Mr. Friedrich was seized pursuant to provisions of the warrant that were particularized and supported by probable cause.⁵ Under the severability doctrine, which “has been applied [even] where First Amendment considerations exist,” “‘infirmity of part of a warrant requires the suppression of evidence seized pursuant to that part of the warrant’ but does not require suppression of anything seized pursuant to valid parts of the warrant.” *Perrone*, 119 Wn.2d at 556 (quoting *United States v. Fitzgerald*, 724 F.2d 633,

⁵ The evidence relied on by the State was found on the Hewlett Packard computer, the Samsung smartphone, the Toshiba computer, and the Micron computer.

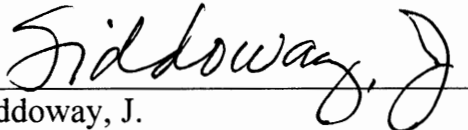
No. 35099-1-III
State v. Friedrich

warrant.” *Perrone*, 119 Wn.2d at 556 (quoting *United States v. Fitzgerald*, 724 F.2d 633, 637 (8th Cir. 1983)). Although the doctrine does not apply to unconstitutional general warrants or where the valid portion of the warrant is “a relatively insignificant part of an otherwise invalid search,” *id.* at 556-57 (internal quotation marks omitted), neither of those exceptions to the doctrine apply here.

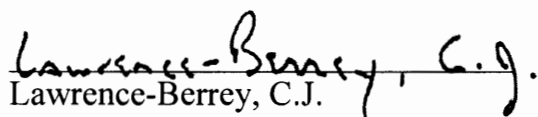
The warrant was not too vague and did not authorize the seizure of items protected by the First Amendment. Its extension to nine unrelated IP addresses and any other debatable overbreadth did not taint its valid and severable authorization to seize the three computers and one smartphone relied on as evidence against Mr. Friedrich.

Mr. Friedrich asks us to exercise our discretion to waive costs on appeal if the State substantially prevails, which it has. We decline to exercise our discretion to waive costs, but this does not prejudice Mr. Friedrich’s right to oppose an award of costs under RAP 14.2.

Affirmed.


Siddoway, J.

WE CONCUR:


Lawrence-Berrey, C.J.

No. 35099-1-III

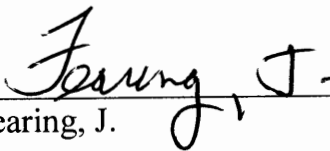
FEARING, J. (concurring) — The majority writes, on page 8 of its opinion:

Whether a warrant affidavit's information constitutes probable cause is a question of law that we review de novo. *State v. Neth*, 165 Wn.2d 177, 182, 196 P.3d 658 (2008). Nonetheless, in determining that question of law, "[g]reat deference is accorded the issuing magistrate's determination of probable cause." *State v. Cord*, 103 Wn.2d 361, 366, 693 P.2d 81 (1985). If the propriety of issuing the warrant is debatable, the deference due the magistrate's decision will tip the balance in favor of upholding the warrant. *State v. Jackson*, 102 Wn.2d 432, 446, 688 P.2d 136 (1984). In light of the deference owed the magistrate's decision, the question on review is whether the magistrate could draw the connection, not whether he should do so.

I question the consistency of the first sentence in this excerpt from the remaining sentences. A de novo review may conflict with granting the magistrate deference, let alone great deference. Perhaps the appeals court should grant deference only to the extent the magistrate needed to determine the reliability of information submitted in support of the application for a search warrant and not to the extent of deciding whether that information supported probable cause. I also question whether a reviewing court should grant the magistrate deference when the magistrate issues the search warrant without any input from the defendant.

No. 35099-1-III
State v. Friedrich (concurrency)

In another case, a court may need to resolve the discrepancy between the principle of de novo review and the rule of granting the magistrate deference. The majority and I need not undertake any resolution of this incongruity in this appeal, because under either standard of review, we may affirm the issuance of the warrant to search Jay Friedrich's residence.



Fearing, J.

BACKLUND & MISTRY

September 24, 2018 - 10:58 AM

Transmittal Information

Filed with Court: Court of Appeals Division III
Appellate Court Case Number: 35099-1
Appellate Court Case Title: State of Washington v. Jay Karl Friedrich
Superior Court Case Number: 16-1-00228-2

The following documents have been uploaded:

- 350991_Motion_20180924105753D3323914_6635.pdf
This File Contains:
Motion 1 - Other
The Original File Name was 350991 State v Jay Friedrich Motion for Overlength Petition.pdf
- 350991_Petition_for_Review_20180924105753D3323914_7076.pdf
This File Contains:
Petition for Review
The Original File Name was 350991 State v Jay Friedrich Petition for Review w Appendix.pdf

A copy of the uploaded files will be sent to:

- backlundmistry1@gmail.com
- jnagle@co.walla-walla.wa.us
- tchen@co.franklin.wa.us

Comments:

Petition for Review Motion for Overlength Petition

Sender Name: Jodi Backlund - Email: backlundmistry@gmail.com
Address:
PO BOX 6490
OLYMPIA, WA, 98507-6490
Phone: 360-339-4870

Note: The Filing Id is 20180924105753D3323914