

No. 35099-1-III

COURT OF APPEALS, DIVISION III  
OF THE STATE OF WASHINGTON

---

STATE OF WASHINGTON,

Respondent,

vs.

**Jay Friedrich,**

Appellant.

---

Walla Walla County Superior Court Cause No. 16-1-00228-2

The Honorable Judge John W. Lohrmann

**Appellant's Opening Brief**

Jodi R. Backlund  
Manek R. Mistry  
Attorneys for Appellant

**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**

**ISSUES AND ASSIGNMENTS OF ERROR..... 1**

**STATEMENT OF FACTS AND PRIOR PROCEEDINGS..... 3**

**ARGUMENT..... 9**

**I. The search warrant application did not establish probable cause because it lacked sufficient facts to assess the allegations for staleness. .... 9**

A. The Court of Appeals must review Mr. Friedrich’s suppression arguments de novo. .... 10

B. The affidavit did not indicate when the unlawful upload occurred, and included no evidence that any device used to upload the image remained at the house nearly a month after Microsoft “became aware” of the upload..... 11

**II. The search warrant was overbroad because it authorized police to search for and seize items for which they lacked probable cause and failed to describe some items with particularity. .... 17**

A. The affidavit did not provide probable cause to search for many items such as books and magazines, and failed to describe numerous articles with particularity. .... 19

B. The affidavit did not provide probable cause to search for anything relating to the nine IP addresses listed in the search warrant. .... 23

**III. If the state substantially prevails, the Court of Appeals  
should decline to award appellate costs. .... 24**

**CONCLUSION ..... 25**

## TABLE OF AUTHORITIES

### FEDERAL CASES

<i>Mapp v. Ohio</i> , 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961).....	12
<i>Stanford v. Texas</i> , 379 U.S. 476, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965) ..	18, 19
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978).....	18

### WASHINGTON STATE CASES

<i>City of Richland v. Wakefield</i> , 186 Wn.2d 596, 380 P.3d 459 (2016)	16, 22
<i>State v. Besola</i> , 184 Wn.2d 605, 359 P.3d 799 (2015) .....	22
<i>State v. Blazina</i> , 182 Wn.2d 827, 344 P.3d 680 (2015).....	24, 25
<i>State v. Gunwall</i> , 106 Wn.2d 54, 720 P.2d 808 (1986) .....	12
<i>State v. Higgs</i> , 177 Wn. App. 414, 311 P.3d 1266 (2013), <i>as amended</i> (Nov. 5, 2013).....	17
<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).....	13, 19
<i>State v. Lamar</i> , 180 Wn.2d 576, 327 P.3d 46 (2014) .....	11
<i>State v. Lyons</i> , 174 Wn.2d 354, 275 P.3d 314 (2012). 10, 12, 13, 14, 15, 16	
<i>State v. Maddox</i> , 116 Wn. App. 796, 67 P.3d 1135 (2003), <i>as amended</i> (May 20, 2003), <i>aff'd</i> , 152 Wn.2d 499, 98 P.3d 1199 (2004).....	17, 19
<i>State v. Meneese</i> , 174 Wn.2d 937, 282 P.3d 83 (2012) .....	12
<i>State v. Neth</i> , 165 Wn.2d 177, 196 P.3d 658 (2008).....	10
<i>State v. O'Hara</i> , 167 Wn.2d 91, 217 P.3d 756 (2009), <i>as corrected</i> (Jan. 21, 2010) .....	11

<i>State v. Perrone</i> , 119 Wn.2d 538, 834 P.2d 611 (1992)..	17, 18, 19, 21, 22, 23, 24
<i>State v. Russell</i> , 171 Wn.2d 118, 249 P.3d 604 (2011).....	10
<i>State v. Swetz</i> , 160 Wn. App. 122, 247 P.3d 802 (2011) <i>review denied</i> , 174 Wn.2d 1009, 281 P.3d 686 (2012).....	10
<i>State v. Thein</i> , 138 Wn.2d 133, 977 P.2d 582 (1999).....	13, 16
<i>State v. White</i> , 135 Wn.2d 761, 958 P.2d 962 (1998).....	12

**CONSTITUTIONAL PROVISIONS**

U.S. Const. Amend. I.....	1, 2, 18, 19, 21, 22, 23
U.S. Const. Amend. IV .....	1, 8, 12
U.S. Const. Amend. XIV .....	12
Wash. Const. art. I, §7.....	1, 8, 12

**OTHER AUTHORITIES**

18 U.S.C. §2258A.....	15
GR 34.....	25
RAP 14.2.....	24, 25
RAP 2.5.....	10, 11

## **ISSUES AND ASSIGNMENTS OF ERROR**

1. The trial court erred by denying Mr. Friedrich's motion to suppress items obtained in violation of his right to be free from unreasonable searches and seizures under the Fourth Amendment.
2. The trial court erred by denying Mr. Friedrich's motion to suppress items obtained in violation of his right to privacy under Wash. Const. art. I, §7.
3. The search warrant was not based on probable cause, because the affidavit failed to provide facts sufficient to allow the issuing magistrate to determine whether the allegations were stale or current.
4. The search warrant was not based on probable cause, because the affiant failed to say when the upload of the suspected image took place.
5. The search warrant was not based on probable cause, because the affiant failed to establish that any device associated with the suspect image remained at the residence nearly a month after Microsoft became aware of the upload.
6. The trial court erred by adopting Finding of Fact No. 1 (CP 85).
7. The trial court erred by adopting Finding of Fact No. 3 (CP 86).
8. The trial court erred by adopting Conclusion of Law No. 2 (CP 87).
9. The trial court erred by adopting Conclusion of Law No. 3 (CP 87).

**ISSUE1:** A search warrant must be based on probable cause. Must the evidence seized be suppressed because the warrant application failed to provide sufficient facts to determine if the allegations of criminal activity were stale?
10. The search warrant was unconstitutionally overbroad.
11. The warrant improperly authorized police to search for and seize items for which they lacked probable cause, including items protected by the First Amendment.
12. The warrant improperly authorized police to search for and seize items that were not associated with criminal activity, including items protected by the First Amendment.

13. The warrant improperly authorized police to search for and examine numerous items unrelated to the single suspect image flagged by Microsoft, including “[a]ny and all books and magazines,” prints and negatives, “[a]ny and all motion picture films, video cassettes, and digital video disks,” “video recordings which are self-produced,” and many other items.
14. The warrant improperly allowed police to search for and seize “[r]ecords and things evidencing the use of” nine IP addresses that were not mentioned in the affidavit and that differed from the one provided by Microsoft.

**ISSUE 2:** A search warrant is unconstitutionally overbroad if it authorizes a search for items for which there is no probable cause. Was the warrant here unconstitutionally overbroad because it authorized police to search for, examine, and seize items protected by the First Amendment in the absence of any evidence suggesting such items existed, would be found at the residence, or would provide evidence of criminal activity?

15. The Court of Appeals should decline to impose appellate costs, should Respondent substantially prevail and request such costs.

**ISSUE 3:** If the state substantially prevails on appeal and makes a proper request for costs, should the Court of Appeals decline to impose appellate costs because Jay Friedrich is indigent, as noted in the Order of Indigency?

## **STATEMENT OF FACTS AND PRIOR PROCEEDINGS**

On April 27, 2016, a Walla Walla police detective named Eric Knudson sought a search warrant for a house in Walla Walla. CP 23-38. The house was occupied by a married couple and their son as well as their housemate Jay Friedrich. CP 24-25, 97.

In his application for the search warrant, Knudson explained how he came to target that house. CP 23-34. About a month earlier, Microsoft had reported it “became aware that a user uploaded a media file believed to contain... suspected” child pornography. CP 23.<sup>1</sup>

Knudson wrote that Microsoft “became aware” of the upload on March 30, 2016 at around 10 a.m. CP 23. However, Knudson did not say when the upload occurred, or what it meant for an entity like Microsoft to become “aware” of internet activity. CP 23-34.

Microsoft provided a single IP (“Internet Protocol”) address associated with the upload. CP 23. Knudson traced the IP address to the house where Mr. Friedrich lived with three others. CP 24. Knudson

---

<sup>1</sup> “Uploading” a file means transferring it from a local computer to a remote system. CP 16. Often this means transferring it from a home computer to a web site. “Downloading” a file means the reverse: transferring it from a remote system to a local computer. CP 16. Often this means copying it from a web site to a home computer. The trial court’s findings erroneously state that “a computer user had *downloaded* a photo...” CP 80, 85 (emphasis added). The record relating to suppression does not support this finding. CP 23-34. The error was also included in Mr. Friedrich’s “Stipulation as to Facts Sufficient for Finding of Guilt,” and the court’s findings on guilt CP 76-77, 80.

explained that relevant information can persist on a hard drive or other storage media for a long time, even after attempts to erase it. CP 26-27. However, he did not provide information showing the computer or other device used to upload the suspect image actually remained at the residence during the month since Microsoft “became aware” of the upload. CP 23-34.

In his request for a warrant, Knudson also made numerous general assertions about “pornographers,” “suspects,” “individuals that trade in this type of illegal activity,” and “child pornography collectors.” CP 13-14. For example, he 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.

Based on this information, a judge granted Knudson a warrant to search the residence. CP 35. The warrant authorized Knudson to search for and seize many types of items. In addition to electronic equipment and storage media, these included:

- a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession,

receipt, or distribution of [child pornography as defined by statute.]

- b. Any and all books and magazines containing [child pornography as defined by statute.]
- c. All originals, copies, and negatives of [child pornography as defined by statute.]
- d. Any and all motion picture films, video cassettes, and digital video disks (“DVDs”) of [child pornography as defined by statute]; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;
- e. Any and all records, documents, or materials, including any and all books, ledgers, and records, relating to the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce (including by United States mail or by computer), of any [child pornography as defined by statute.]
- f. Any and all records, documents, or materials, including any and all address books, names, and lists of names and address of minors visually depicted [in child pornography as defined by statute.]
- g. As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications, or materials created, modified, or stored in any form.

CP 35-36.

Knudson's affidavit did not include any evidence relating to child pornography other than the single digital uploaded image flagged by Microsoft.<sup>2</sup> CP 23-34.

Knudson did not provide any information suggesting that Mr. Friedrich had nondigital images such as photographic prints or negatives. CP 23-34. Nor did the affidavit include any evidence that movies or videos, whether digital or otherwise, would be found at the residence. CP 23-34. The suspect image was uploaded to Skype; however, the affidavit provided no information suggesting another person received the image. Furthermore, other than this single instance, there was no hint that Mr. Friedrich corresponded with anyone about child pornography. CP 23-34.

Nothing in the affidavit showed that Mr. Friedrich created or "self-produced" child pornography images or videos, or that there would be videos, names, addresses, or any other information that would help locate child victims of exploitation or abuse. CP 23-34. Nor did the warrant application include evidence that Mr. Friedrich would have "books, ledgers, and records, relating to the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce" of child

---

<sup>2</sup> Years earlier, Mr. Friedrich's roommate had reported inappropriate images on Mr. Friedrich's laptop; however, a police investigation yielded no charges. CP 24.

pornography, other than record of the single Skype upload flagged by Microsoft. CP 23-34, 36.

Among the “digital evidence” to be seized, the warrant listed “personal digital assistants [and] wireless communication devices such as telephone paging devices [and] beepers.” CP 36. It also listed “peripheral input/output devices such as keyboards, printers, scanners, plotters, [and] monitors,” as well as “communications devices such as modems, routers, cables, and connections... and security devices.” CP 36. The warrant also authorized seizure of “documentation... and reference manuals” for devices and software found at the residence. CP 36.

The warrant application did not provide evidence supporting the existence of many of these items. Nor did it explain why it would be necessary to seize (for example) the keyboards and computer reference manuals found at the residence. CP 23-34.

Although Microsoft identified only one IP address associated with the suspect upload, the warrant authorized police to search for and seize “Records and things evidencing the use of” nine different IP addresses.<sup>3</sup> CP 37. The IP address provided by Microsoft was not among the nine listed in the warrant. CP 37. Included in the list of “Records and things”

---

<sup>3</sup> These nine IP addresses do not appear elsewhere in the materials. They may be left over verbiage from a previous search warrant, unrelated to this case.

were “records of Internet activity, including firewall logs, caches, browser history and cookies, ‘bookmarked’ or ‘favorite’ web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.” CP 37.

The warrant application acknowledged that the premises would likely contain computers and other devices used and owned by “persons who are not suspected of a crime.” CP 29. However, Knudson believed the warrant “would permit the seizure and review of those items as well.” CP 29.

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.

Without hearing argument, the court denied the motion. 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.<sup>4</sup> CP 76-84.

---

<sup>4</sup> It does not appear that Mr. Friedrich waived his right to a jury trial, either orally or in writing. RP 3-6; CP 76-79. If he wishes to challenge the stipulation, appellate counsel will seek permission to file a supplemental brief.

Because each count added three points to his offender score, Mr. Friedrich was sentenced with an offender score of 12.<sup>5</sup> CP 103. The court imposed 95 months in prison. CP 106.

The sentencing judge concluded that Mr. Friedrich had the ability or likely future ability to pay “the legal financial obligations ordered herein.” CP 104. Yet these financial obligations included only mandatory amounts, totaling \$800. CP 104. The court found Mr. Friedrich indigent and authorized him to appeal at public expense. CP 120. Mr. Friedrich timely appealed. CP 41.

## **ARGUMENT**

### **I. THE SEARCH WARRANT APPLICATION DID NOT ESTABLISH PROBABLE CAUSE BECAUSE IT LACKED SUFFICIENT FACTS TO ASSESS THE ALLEGATIONS FOR STALENESS.**

Nearly a month after Microsoft made its report, Detective Knudson applied for a search warrant. CP 23, 30. Knudson did not say when the suspect upload occurred; instead, without explanation, he gave the date Microsoft “became aware” of the upload. CP 23. No evidence suggested that the device used to upload the suspect image remained at the house during the month following the report and the warrant application. CP 23-34.

---

<sup>5</sup> His only prior felony offense—second-degree assault with sexual motivation, committed in 2001—had washed out. CP 103.

Knudson's affidavit did not provide probable cause. *State v. Lyons*, 174 Wn.2d 354, 359-363, 275 P.3d 314 (2012). The issuing magistrate had no way of knowing when the criminal activity occurred or if evidence remained at Mr. Friedrich's residence. *Id.* The items and images seized should have been suppressed. *Id.*

A. The Court of Appeals must review Mr. Friedrich's suppression arguments *de novo*.

Like all constitutional issues, the validity of a search warrant is an issue of law reviewed *de novo*. *State v. Neth*, 165 Wn.2d 177, 182, 196 P.3d 658 (2008).

Mr. Friedrich's motion to suppress should be sufficient to preserve all arguments supporting exclusion of the evidence. CP 5. Furthermore, even if unpreserved, the arguments raised on appeal may be considered for the first time on review under RAP 2.5(a)(3).

The introduction into evidence of material unconstitutionally seized creates a manifest error affecting a constitutional right.<sup>6</sup> RAP 2.5(a)(3); *State v. Swetz*, 160 Wn. App. 122, 128, 247 P.3d 802 (2011) *review denied*, 174 Wn.2d 1009, 281 P.3d 686 (2012). To raise a manifest

---

<sup>6</sup> The court may also accept review of other issues argued for the first time on appeal, including constitutional errors that are not manifest. RAP 2.5(a); *see State v. Russell*, 171 Wn.2d 118, 122, 249 P.3d 604 (2011).

constitutional error, an appellant need only make “a plausible showing that the error... had practical and identifiable consequences in the trial.” *State v. Lamar*, 180 Wn.2d 576, 583, 327 P.3d 46 (2014).<sup>7</sup>

An error has practical and identifiable consequences if “given what the trial court knew at that time, the court could have corrected the error.” *State v. O'Hara*, 167 Wn.2d 91, 100, 217 P.3d 756 (2009), *as corrected* (Jan. 21, 2010). In this case, the erroneous admission of illegally seized evidence had practical and identifiable consequences. *Id.* Without the evidence, the State would have been unable to proceed to trial.

Furthermore, the court had a copy of the warrant affidavit and the search warrant, and “could have corrected the error” by suppressing the evidence on any proper grounds. *Id.* The arguments presented here may be raised for the first time on appeal, if they are not sufficiently preserved by Mr. Friedrich’s motion to suppress. *Id.*

- B. The affidavit did not indicate when the unlawful upload occurred and included no evidence that any device used to upload the image remained at the house nearly a month after Microsoft “became aware” of the upload.
  - 1. A search warrant must be based on probable cause and may not rest on generalizations about the habits of criminal suspects.

---

<sup>7</sup> The showing required under RAP 2.5(a)(3) “should not be confused with the requirements for establishing an actual violation of a constitutional right.” *Id.*

The Fourth Amendment protects against unreasonable searches and seizures. U.S. Const. Amend. IV.<sup>8</sup> The state constitution protects against disturbance of a person’s private affairs or invasion of a person’s home without authority of law. Wash. Const. art I, §7. It provides stronger protection to individual privacy rights than does the Fourth Amendment.<sup>9</sup> *State v. Meneese*, 174 Wn.2d 937, 946, 282 P.3d 83 (2012).

Under both constitutional provisions, search warrants must be based on probable cause. *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.*

An affidavit in support of a search warrant “must state the underlying facts and circumstances on which it is based in order to facilitate a detached and independent evaluation of the evidence by the issuing magistrate.” *State v. Thein*, 138 Wn.2d 133, 140, 977 P.2d 582 (1999). By itself, an inference drawn from the facts “does not provide a

---

<sup>8</sup> The Fourth Amendment is applicable to the states through the action of the Fourteenth Amendment. U.S. Const. Amend. XIV; *Mapp v. Ohio*, 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961).

<sup>9</sup> 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).

substantial basis for determining probable cause.” *Lyons*, 174 Wn.2d at 363-64. Conclusory statements of an affiant’s belief do not support a finding of probable cause. *Id.*, at 365.

Similarly, generalizations about what criminals generally do cannot provide the individualized suspicion required to justify the issuance of a search warrant. *Thein*, 138 Wn.2d at 147-148. The constitution requires more. *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).

2. The search warrant was not based on probable cause, because the allegations were stale and involved generalizations about the habits of criminal suspects.

Stale information cannot establish probable cause. *Lyons*, 174 Wn.2d at 359-363. When assessing staleness, 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. 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 included the first of these critical moments, but omitted the second: “Within the last 48 hours a reliable and

confidential source of information (CS) contacted [narcotics] 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 concluded 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.

The affidavit in this case suffers from the same defect.<sup>10</sup> *Lyons* controls, because the affidavit does not “provide sufficient support for the magistrate’s finding of *timely* probable cause.” *Id.* (emphasis added).

Knudson’s warrant application shows “Microsoft reported... that on March 30, 2016 at 10:04:17 hours UTC *they became aware* that a user uploaded a media file” suspected to contain child pornography. CP 23 (emphasis added). Although Microsoft “became aware” of the upload just after 10 a.m. on March 30<sup>th</sup>, nothing in the warrant application shows

---

<sup>10</sup> In fact, the flaw here is more serious than in *Lyons* because it is not clear the informant (Microsoft) knew or told Knudson when the criminal activity transpired.

when the upload occurred. CP 23.<sup>11</sup>

Nor does the affidavit explain what it means for an entity like Microsoft to “become aware” of internet activity. For example, it is possible that the upload occurred days or weeks earlier, and Microsoft did not become “aware” of it until a technician reviewed information previously flagged by the company’s software.

Absent this information, the affidavit does not establish probable cause. *Lyons*, 174 Wn.2d. at 363. As in *Lyons*, the affidavit lacks a critical piece of 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” consisted of a single image upload.<sup>12</sup> *Lyons*, 174 Wn.2d at 361. Nothing in

---

<sup>11</sup> An Electronic Service Provider or Internet Service Provider must report child pornography “as soon as reasonably possible.” CP 18 (citing 18 U.S.C. §2258A(a)(1)). Presumably, Microsoft complied with this requirement by providing the information shortly after they “became aware” of the upload. However, nothing in the affidavit indicates how long it takes an entity like Microsoft to “become aware” of an illegal upload after the upload transpires.

<sup>12</sup> As noted previously, uploading a file means transferring it from a local computer to a remote system. Downloading a file means the reverse: transferring it from a remote system to a local computer. CP 16. The trial court erroneously found that Knudson received a report “that a user had downloaded a photo.” CP 85. This finding is not supported by the evidence: the warrant affidavit makes clear that Microsoft reported the *upload* of an image. CP 23. The finding must be stricken. *See, e.g., City of Richland v. Wakefield*, 186 Wn.2d 596, 610, 380

the warrant application 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).

It is irrelevant that information persists on electronic media, as Knudson outlines at length. CP 26-27. Computers, hard drives, and other such devices are highly portable. As time passes, the likelihood of the electronic media leaving the premises increases.

Nor do Knudson’s statements about the general habits of “child pornography collectors” establish probable cause. CP 13-15. Such “blanket inferences” and “generalities” do not show that the person who uploaded the single suspect image in this case would keep it “for many years” or would “prefer not to be without [it] for any prolonged time period.” CP 15; *Thein*, 138 Wn.2d at 147.

*Lyons* requires suppression. *Lyons*, 174 Wn.2d at 359-363.

Knudson’s search warrant affidavit lacked crucial information and did not provide probable cause to search the residence. Without knowing when the upload occurred, the issuing magistrate could not know if any device or media containing the single uploaded image remained at the place to be

---

P.3d 459 (2016) (“There is no evidence to support this finding of fact and, therefore, we strike it.”)

searched. *Id.*

Mr. Friedrich's convictions must be reversed, the evidence suppressed, and the charges dismissed with prejudice. *Id.*

**II. THE SEARCH WARRANT WAS OVERBROAD, BECAUSE IT AUTHORIZED POLICE TO SEARCH FOR AND SEIZE ITEMS FOR WHICH THEY LACKED PROBABLE CAUSE AND FAILED TO DESCRIBE SOME ITEMS WITH PARTICULARITY.**

A search warrant is overbroad if it authorizes police to search for or seize items for which they lack probable cause. *State v. Higgs*, 177 Wn. App. 414, 426, 311 P.3d 1266, 1273 (2013), *as amended* (Nov. 5, 2013); *State v. Maddox*, 116 Wn. App. 796, 805, 67 P.3d 1135, 1140 (2003), *as amended* (May 20, 2003), *aff'd*, 152 Wn.2d 499, 98 P.3d 1199 (2004). A warrant is overbroad even if probable cause supports some portions of the warrant. *Higgs*, 177 Wn. App. at 426.

A warrant is also 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). The probable cause and particularity requirements are "closely intertwined." *Id.* 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.

For example, in *Perrone*, the court found a search warrant “overly broad in its entirety.” *Perrone*, 119 Wn.2d at 542. One problem was the warrant used the phrase “child pornography,” which the Supreme Court found too vague to meet the particularity requirement. *Id.*, at 553. The court reasoned that this language 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 the “scrupulous exactitude” required for seizure of materials presumptively protected by the First Amendment. *Id.*

The second problem with the *Perrone* warrant was that it authorized a search for some items for which the police lacked probable

cause.<sup>13</sup> *Perrone*, 119 Wn.2d at 551-52. This contributed to the court’s finding that the warrant was overbroad. *Id.*, at 558.<sup>14</sup>

Here, as in *Perrone*, Knudson sought materials presumptively protected by the First Amendment. In evaluating the warrant, the particularity requirement must be “accorded the most scrupulous exactitude.” *Perrone*, 119 Wn.2d at 547–48 (quoting *Stanford*, 379 U.S. at 485).

A. The affidavit did not provide probable cause to search for many items such as books and magazines, and failed to describe numerous articles with particularity.

Detective Knudson received information regarding a single digital image. CP 23. Despite this, he sought and received authorization to search for “books and magazines,” “motion picture films, video cassettes, and digital video disks,” “video recordings,” and a great deal of additional material that he speculated might be present. CP 35-36.

---

<sup>13</sup> 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.

<sup>14</sup> Similarly, in *Maddox*, the warrant “authorized the police to search for a number of items that were supported by probable cause,” including drugs, paraphernalia, and records showing drug distribution and profits. *Maddox*, 116 Wn. App. at 806. However, the court found the warrant overbroad because it also authorized a search “for many items for which there was no probable cause whatever: books and records showing ‘the identity of co-conspirators’; photographs of co-conspirators, assets, and drugs; and other books and records not associated with methamphetamine distribution.” *Id. see also Keodara*, 191 Wn. App. at 316 (“[T]he warrant’s language also allowed Keodara’s phone to be searched for items that had no association with any criminal activity and for which there was no probable cause whatsoever.”)

Furthermore, contrary to the trial court’s findings, only some of the “item[s] to be searched or seized included language limiting the search to” child pornography as defined by statute. CP 86. In fact, none of the items listed under the heading “Digital Evidence” included this limitation. CP 36-37.

Instead, for example, the warrant authorized seizure of “[a]ll computers, including *any electronic or digital device capable of storing and/or processing data in digital form,*” without any limitation. CP 36 (emphasis added). This language and the accompanying list show the extraordinary breadth of the authority granted by the warrant. CP 36. The warrant authorized seizure of any device with a chip—a digital thermometer, for example—even if it were immediately apparent the device had no connection to the suspect image or to child pornography generally. CP 36.

The same is true of the other provisions under the “Digital Evidence” heading. Among other things, the overlapping categories covered any equipment used for creation, display, storage, or transmission of digital data, as well as software, and reference manuals. None of these provisions contain the limiting language referenced by the court in its findings. CP 86.

One provision allows seizure of “[a]ll records, documents, [etc]” that identify the user when the computer was used to “upload, download, store, receive, possess or view child pornography.” CP 37.<sup>15</sup> As in *Perrone*, the reference to “child pornography” fails the particularity requirement: “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.

The items listed under “Digital Evidence” were not described with particularity. Unlike the other provisions of the warrant, the section on “Digital Evidence” authorized police to seize broad categories of property protected by the First Amendment, without any limitations. CP 36-37. It is irrelevant that the statutory language was included elsewhere in the warrant. *See State v. Besola*, 184 Wn.2d 605, 614, 359 P.3d 799 (2015).

Police were permitted to seize anything that fit within the broad categories listed under the heading “Digital Evidence,” even if unrelated to the commission of any crime. These provisions did not include the limiting language set forth elsewhere in the warrant. CP 36-37. The items listed under “Digital Evidence” were not described with “scrupulous

---

<sup>15</sup> The paragraph goes on to clarify this includes browser history, temporary internet files, email, instant messages, and numerous other categories of information protected by the First Amendment. CP 37.

exactitude.” *Perrone*, 119 Wn.2d at 553. Furthermore, the absence of any reference to the statutory definition of child pornography means that Finding No. 3 is not supported by substantial evidence and must be vacated. CP 86; *Wakefield*, 186 Wn.2d at 610.

The warrant was overbroad, because it was not based on probable cause, and it failed the particularity requirement. Knudson provided no facts suggesting the house would contain anything more than the single digital image flagged by Microsoft. CP 23-34. Nothing in the warrant application shows the police could expect to find books or magazines containing child pornography, or any other materials not directly tied to the digital image. CP 23-34. Furthermore, officers were empowered to seize broad categories of items protected by the First Amendment, without limitation. CP 35-37. The “Digital Evidence” to be seized was not described with scrupulous exactitude. *Perrone*, 119 Wn.2d at 553.

Although police had information about a single digital image, the warrant permitted them to rummage through all of Mr. Friedrich’s books, magazines, movies, and other possessions. CP 35-36. It permitted seizure of items completely unrelated to any criminal activity, including items protected by the First Amendment. CP 36-37.

The warrant was unconstitutionally overbroad. *Id.*, at 542. The evidence should have been suppressed. *Id.* Mr. Friedrich’s convictions

must be reversed, the evidence suppressed, and the case dismissed with prejudice. *Id.*

B. The affidavit did not provide probable cause to search for anything relating to the nine IP addresses listed in the search warrant.

Microsoft provided a single IP address: 96.39.147.251. CP 23. The entire warrant application depended on the connection Knudson drew between this IP address and the Pine Street residence. CP 23-25.

Despite this, the search warrant authorized police to search for and seize “[r]ecords and things evidencing the use of” nine different IP addresses, none of which were the IP address provided by Microsoft. CP 37.<sup>16</sup> The affidavit did not mention, much less establish probable cause, to search for or seize any records or other items relating to these nine IP addresses.<sup>17</sup> CP 23-34.

The search warrant was overbroad. *Perrone*, 119 Wn.2d at 547. The court should have suppressed the evidence. *Id.* Mr. Friedrich’s convictions must be reversed, the evidence suppressed, and the case dismissed with prejudice. *Id.*

---

<sup>16</sup> Furthermore, Appendix B to the affidavit lists two additional IP addresses: 97.115.128.137 and 97.15.177.237. CP 33. The body of the affidavit makes no reference to these two addresses.

<sup>17</sup> It is not at all clear where the nine IP addresses came from. They do not appear elsewhere in the materials. It is possible they are residue Knudson failed to delete from a prior search warrant.

**III. IF THE STATE SUBSTANTIALLY PREVAILS, THE COURT OF APPEALS SHOULD DECLINE TO AWARD APPELLATE COSTS.**

The Court of Appeals should decline to award appellate costs, because Jay Friedrich “does not have the current or likely future ability to pay such costs.” RAP 14.2. The concerns identified by the Supreme Court in *Blazina* apply with equal force to this court’s discretionary decisions on appellate costs. *State v. Blazina*, 182 Wn.2d 827, 344 P.3d 680 (2015).

The trial court found Jay Friedrich indigent. CP 120. That status is unlikely to change, especially with the addition of five convictions relating to child pornography. CP 102-103.

Although the sentencing judge found Mr. Friedrich had the ability or likely future ability to pay mandatory LFOs, the court did not impose any discretionary LFOs. CP 104. Mr. Friedrich has worked steadily, but has never held a high-paying job, and he had bills in collections at the time of his arrest. CP 93-95.

The *Blazina* court indicated that courts should “seriously question” the ability of a person who meets the GR 34 standard for indigency to pay discretionary legal financial obligations. *Id.* at 839. Here, the trial court’s finding of indigency “remains in effect.” RAP 14.2.

If the state substantially prevails on this appeal, this court should deny any appellate costs requested. RAP 14.2.

**CONCLUSION**

For the foregoing reasons, Mr. Friedrich's convictions must be reversed. The evidence must be suppressed, and the case dismissed with prejudice. If the state substantially prevails, the Court of Appeals should decline to impose appellate costs.

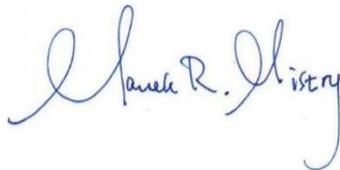
Respectfully submitted on July 24, 2017,

**BACKLUND AND MISTRY**



---

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



---

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

CERTIFICATE OF SERVICE

I certify that on today's date:

I mailed a copy of Appellant's Opening Brief, postage prepaid, to:

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

With the permission of the recipient(s), I delivered an electronic version of the brief, using the Court's filing portal, to:

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

I filed the Appellant's Opening Brief electronically with the Court of Appeals, Division III, through the Court's online filing system.

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 July 24, 2017.



---

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

# BACKLUND & MISTRY

July 24, 2017 - 3:30 PM

## 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\_Briefs\_20170724152703D3009336\_3630.pdf  
This File Contains:  
Briefs - Appellants  
*The Original File Name was 350991 State v Jay Friedrich Opening Brief.pdf*

### A copy of the uploaded files will be sent to:

- jnagle@co.walla-walla.wa.us
- tchen@co.franklin.wa.us

### Comments:

Appellant's Opening Brief

---

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 20170724152703D3009336**